



## CHAIR'S SUMMARY

### DE-ESCALATION IN CYBERSPACE – MEDIATION AND PREVENTIVE DIPLOMACY Zug, 29 – 30 September 2026

The conference, organised by the Swiss OSCE Chairpersonship in Zug from 29–30 September 2026, brought together over 120 participants from 47 OSCE participating States and 2 Partners for Co-operation, alongside a wide range of representatives from the OSCE Secretariat, academia, the private sector and civil society.

The conference was opened by Federal Councillor Martin Pfister, Head of the Federal Department of Defence, Civil Protection and Sport. He emphasized that preventive diplomacy, communication, and mediation can stop cyber incidents from escalating into wider political or security crises by creating time and space for dialogue and restraint. Welcome remarks were delivered by Ambassador Hatun Demirer, Director of the office of the OSCE Secretary General, followed by a keynote address by Florian Schütz, Director of the Swiss National Cyber Security Center. The opening segment was followed by panel discussions involving practitioners, experts and policymakers. A scenario-based discussion enabled the participants to address the challenges of managing cyber incidents and preventing escalation.

The three panel sessions focused on existing consultation and confidence-building measures, cyber mediation as an emerging tool for de-escalation, how non-state actors can support states and help prevent escalation and the role of emerging technologies in supporting stability and resilience in cyberspace.

Raphael Nägeli, the Permanent Representative of Switzerland, summarised key findings. Federal Councillor Ignazio Cassis, the OSCE Chairman-in-Office provided closing remarks. He emphasised that the challenges to prevent escalation in cyberspace are not only technological, but diplomatic, and ultimately human. He stressed that this is where the OSCE matters, offering a table around which adversaries can talk. The Canton of Zug hosted an official reception that included a presentation of the Canton of Zug's cybersecurity initiative. A variety of side events offered attendees the opportunity to experience the thematic breadth of the Zurich-Zug innovation environment.



**DIALOGUE  
TRUST  
SECURITY**

## Purpose and context

Artificial intelligence, quantum computing and digital connectivity are transforming our societies at unprecedented speed. Cyberspace has become a new domain of strategic competition, bringing immense opportunities but also new vulnerabilities. At a time of growing geopolitical tensions, ensuring that technological change contributes to stability rather than insecurity is a shared responsibility

This reality is particularly relevant in cyberspace. Cyber incidents can spread across borders within seconds, affect critical infrastructure and generate tensions whose origins are often difficult to establish with certainty. In such circumstances, the risk lies not only in an incident itself, but in how it is perceived and how states react to it. For its 2026 Chairpersonship of the OSCE, Switzerland made inclusive multilateralism a priority, encouraging cooperation on cybersecurity and conflict prevention.

The objective of this conference was to discuss existing and potential threats in cyberspace, identify ways to avoid escalation and conflict in the event of serious cyber incidents through consultation and mediation, and examine the role non-state actors and digital technologies can play in conflict prevention.

The event took place in Zug. The Zurich-Zug region is one of Switzerland's most dynamic innovation environments, bringing together world class research, universities, technology companies and startups, with particularly strong ecosystems in AI, ICT and cybersecurity.

## Content

The opening high-level segment highlighted that in an era of rapid transformation, the challenge is not only technological, but equally diplomatic. Opening the conference, Federal Councillor Martin Pfister put it plainly: "We cannot prevent every cyber incident. But we can work to prevent cyber incidents from becoming a crisis." He was joined by Ambassador Hatun Demirer, Director of the Office of the OSCE Secretary General, who highlighted the OSCE's role in preventing escalation in cyberspace, stressing the importance of keeping its confidence-building measures operational and adapted to evolving technologies. In his keynote speech Florian Schütz examined the impact of geopolitical and technological developments on cybersecurity.

In-depth sessions focused on three themes:

### Mechanisms for timely consultations following cyber incidents

The session explored how preventive diplomacy can help identify and address cyber-related tensions before they escalate into political crises. Participants highlighted the importance of early warning, anticipation and timely com-

munication, including the effective use of existing OSCE confidence-building measures. Greater cooperation between cybersecurity authorities, diplomats, and security institutions was seen as essential to understand emerging risks and creating space for dialogue. The panel also considered how AI and other emerging technologies may accelerate cyber incidents and increase the risk of miscalculation, underlying the need to anticipate technological developments as part of preventive diplomacy.

### Cyber mediation as an emerging tool for de-escalation

The discussion examined the role of mediation and de-escalation in responding to cyber incidents with potential political or security consequences. Participants stressed that trusted communication channels, clarification and confidence-building can help prevent misunderstandings from escalating. Effective cyber mediation requires both technical understanding and diplomatic expertise, as well as ability to engage relevant actors rapidly. The discussion emphasised the importance of developing mediation capacities before crisis occur and using practical exercises to test diplomatic responses. The OSCE was recognised as a useful platform for dialogue and for strengthening approaches to cyber crisis management.

### The contribution of non-state actor expertise

This panel focused on the contribution of the private sector, technical communities, academia and civil society to preventing and managing cyber crises. Non-state actors can provide valuable early warning, technical expertise and situational awareness, often detecting developments before governments have a complete picture. Participants discussed the need for structural and trusted channels of engagement that allow such expertise to inform diplomatic decision-making while maintaining the central role of states. The panel also highlighted the growing importance of cooperation with technology companies and experts in anticipating the opportunities and risks arising from AI and other emerging technologies.

### Scenario-based discussion

The scenario involved three fictional countries, each affected differently by a vulnerability in a software component that is part of their respective AI supply chains. The scenario presented numerous opportunities for misunderstandings. Participants were presented with new information in rapid succession. The groups communicated via an electronic platform designed to simulate the OSCE Communication Network. The participants discovered that perception and reality do not always align, and that the tense situation could only be defused by acting together and sharing information.

## Recommendations

### To OSCE participating States

1. Regularly update and practice OSCE communication channels and Points of Contact to ensure they remain operational, trusted and ready for use during emerging cyber crises.
2. Use existing OSCE confidence-building measures proactively for early warning, information-sharing, clarification and de-escalation, before cyber incidents develop into political crises.
3. Strengthen national capacities for preventive diplomacy and mediation in cyberspace by connecting cyber, foreign policy, security and crisis-management expertise.
4. Establish structured channels with the private sector, academia and civil society to strengthen early warning, technical understanding, situational awareness and crisis prevention.
5. Integrate technological anticipation into preventive diplomacy by assessing and sharing how AI and emerging technologies may transform cyber risks, escalation dynamics and crisis management.

### To the OSCE executive structures

1. Facilitate regular exercises of OSCE communication mechanisms and Points of Contact to strengthen preparedness, trust and practical crisis-management capacity.
2. Strengthen OSCE anticipation and early warning capacities through horizon-scanning, expert exchanges and scenario discussions on emerging cyber risks and escalation dynamics.
3. Further develop the OSCE's role in cyber mediation and de-escalation by strengthening cooperation between cyber and conflict-prevention expertise, including through practical guidance, exchanges of experience and scenario-based exercises.
4. Strengthen structured engagement with private-sector, technical, academic and civil-society stakeholders to enhance situational awareness and support preventive diplomacy.
5. Connect technological foresight with practical preventive diplomacy by assessing AI and emerging technologies and translating identified risks and opportunities into appropriate confidence-building measures and guidance.



Federal Councillor Martin Pfister



Federal Councillor Ignazio Cassis, OSCE Chairman-in-Office



Panel discussion



Participants in the OSCE Conference "De-Escalation in Cyberspace"