

«Cybersecurity is a shared responsibility - of the state, the economy and society»

Datum 29.9.2026
Subjekt Eidgenössisches Departement für auswärtige Angelegenheiten EDA
Autor Martin Pfister
Region Switzerland
Kategorie IT, International organizations, Security

Zug, 29.09.2026 — Eröffnungsansprache von Bundesrat Martin Pfister, Chef des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS), anlässlich der am Dienstag, 29. September 2026, unter Schweizer Vorsitz stattfindenden OSZE-Konferenz in Zug.

Es gilt das gesprochene Wort

Distinguished Guests,
Delegations from OSCE Participating States,
Excellencies, Ladies and gentlemen,

It is a great pleasure to welcome you here in Zug.

There are good reasons why we have chosen this location to discuss de-escalation in cyberspace.

First, Zug is my home – and by far Switzerland's most beautiful region, as I am sure you will all agree.

But there are more objective reasons as well.

The Zurich-Zug region is one of Switzerland's most dynamic centres of innovation.

Zurich brings together world-class research institutions, universities, technology companies and start-ups, with particular strengths in AI, ICT and cybersecurity.

Zug adds another important dimension.

It is a place where technology, entrepreneurship and public policy come together. The Canton is making cybersecurity a strategic priority.

Its Cybersecurity initiative aims to establish a cantonal competence centre for cybersecurity, strengthen the cyber resilience of SMEs, raise awareness among the population, and connect public and private partners. It also envisages strategic cooperation with ETH Zurich and the Lucerne University of Applied Sciences and Arts.

This reflects a broader principle: Cybersecurity is a shared responsibility – of the state, the economy, and society.

This is precisely the kind of ecosystem this conference needs.

Because we are not here only to talk about cybersecurity. We are here to bring together security

expertise, diplomacy, technology and innovation - at a time when the digital and geopolitical worlds have become inseparable.

Cyber incidents can disrupt critical infrastructure, affect public services, compromise sensitive information or undermine trust in institutions.

And they can unfold at extraordinary speed – across borders and often without clear attribution.

Those of us responsible for security and defence have our job to do: We need strong cyber defences. We need resilience. We need the capacity to deter malicious behaviour.

But we also need something else: We need the diplomatic tools that prevent a cyber incident from becoming a wider political or security crisis.

Uncertainty in attribution can easily become escalation.

Evidence can be incomplete, attackers can hide behind third-party infrastructure, and intentions may be unclear.

If we react before we understand what has happened, one incident can trigger another – and escalation can quickly become a cycle of retaliation.

This is why de-escalation must be an integral part of our approach to cyber security.

The question at the heart of our conference is therefore:

How do we prevent a cyber incident from becoming a wider political or security crisis?

There are two important answers to this question: preventive diplomacy and mediation.

In cyberspace, preventive diplomacy means establishing channels of communication before they are needed. It means exchanging information, building confidence and clarifying intentions.

A point of contact may look like a technical detail in normal times. In a crisis, it can become a strategic asset.

Governments cannot undertake this task alone. Much of the world's digital infrastructure is privately owned or operated. And much of the relevant expertise lies in companies, universities and technical communities. Cooperation with these actors is indispensable. They can provide early warning and technical expertise, help establish facts and strengthen resilience.

Cybersecurity is a shared responsibility – of the state, the economy and society.

The OSCE's cyber confidence-building measures are particularly important in this respect. The United Nations framework for responsible State behaviour provides another essential foundation.

But prevention will not eliminate every crisis. There will be cyber incidents where attribution is disputed, political disagreements persist, and trust has already broken down.

This is where the second answer comes in: mediation. Mediation creates a process through which parties can manage disagreement without allowing it to escalate. Dialogue is not a reward for agreement. It is a tool for managing disagreement.

In cyberspace, mediation can help create something extremely valuable: time.

Time to establish facts. Time to clarify intentions. Time to separate technical events from political interpretations. And time for decision-makers to consider whether the next step should be escalation or restraint.

Excellencies,
Ladies and gentlemen,

We cannot prevent every cyber incident.

But we can work together to prevent cyber incidents from becoming wider crises.

Ultimately, de-escalation is about preserving choices.

Security policy must ensure that we are able to defend ourselves. Diplomacy must help ensure that, even under pressure, alternatives remain available.

It creates space between an incident and a reaction. And in that space, there can be verification, communication and restraint.

This is why preventive diplomacy and mediation matter to security. And this is why our discussion today matters.

I wish you a productive conference, frank discussions and, above all, new ideas for keeping communication open precisely when the pressure to close it is greatest.

Thank you.

<https://www.eda.admin.ch/de/newsb/uDGmflnMH3zP>