Personal Invitation to 38th Swiss CISO Summit

swissciso summit

Geopolitical tensions: How to prepare ICT operations when conflicts intensify?

17th September 2026 Haus der Universität Bern
(upon request, virtual participation will be organized)

Sponsorships:

Platinum: Detecon

Gold: pwc

Silver: Hochschule Luzern; Swiss Post

Partner: satw – It's all about technology

Contents

1 Introduction

Dear CISO,

You are kindly invited to the 38th Swiss CISO Summit – a series of moderated round-table discussions for sharing information security practices and strategies among senior professionals.

Please be informed that we have only a limited number of places. Therefore we kindly ask you to confirm your attendance as soon as possible.

Prof. Dr. Bernhard M. Hämmerli

Geopolitical tension: How to prepare ICT-reaction when conflicts intensify?	
Date	17th September 2026, Haus der Universität Bern
Time	12:00 to 19:00h
Location	Haus der Universität Bern, Schlösslistrasse 5, 3008 Bern
Keynote I	**Enterprise Security Risk Management (ESRM): A Converged Approach to Security Governance** Dr. Doron Zimmermann, Principal, Security Risk Management, EPAM
Keynote IIa and IIb	**A production camp in Ukraine – preparation-incidents-lessons identified** Markus Müller-Fehrenbach, CISO Vetropack **Cyber defence of critical infrastructure under armed conflict: Lessons from the Russian–Ukrainian war** Onysiia Kutsovol, Expert from Ukraine
Key Benefits	• Experience industry best practices in the Swiss market • Participate actively in moderated high-level peer exchange • Understand drivers for security, gain competence and experience in discussing strategic issues • Design, develop and manage effective information security strategies for your own organisation • Receive an exclusive consolidated end of summit report detailing all the major themes discussed for re-use in your organization

Join the Swiss CISO Summit and benefit from the peer exchange!

Summary 2

Geopolitical tension: How to prepare ICT-reaction when conflicts intensify?

Our generation has experienced a long period of peace time, and life was calculable, and success depended on our own behavior. With Russia's attack on Ukraine, Europe was confronted with a new reality: war is no longer unimaginable but has become a real possibility that must be considered. Politicians needed time to understand this new reality: before the attack, those who considered war a realistic possibility were often dismissed.

However, international and globally operating companies had to turn around quickly, because today war is a reality in Ukraine, Iran, and all near east; around Taiwan, the political situation is tense. In these areas, war has unfortunately become a sad reality. Putin said recently that a limited attack against NATO states is for him an option in the next 2–3 years. He believes that, after testing with many small incidents, he will get away with such an operation without a large-scale war.

Against this background, the topic of ICT operations in times of growing political tension and in war areas is of paramount importance for large companies and should be taken seriously.

In conclusion, war readiness of ICT operations is complex, and must have a sound balance between organization (what we can do up front) and improvisation (what is case-specific, and we cannot plan). However, Compliance and Frameworks are still important and a “must” through all situations, including war. Just as in most difficult times, a balance between functionality and compliance is needed– in this case, operation and functionality are more important.

Key benefits are often declared as follows:

- Extended view on resilience, including war and war-like situations.
- Understanding that political conflicts must be observed, and in case of escalating conflicts, the CISO must understand that a new dimension of preparedness is needed. At this time, it is probably more about sites in or near conflict zones, but escalation might be very fast, as we experienced with the Russian attack on Ukraine, February 24, 2022.
- Understanding in-depth why improvisation is an utmost important capability in ICT operations in warlike situations.

2 Summary

Doron Zimmermann, Principal, Security Risk Management, EPAM, will give a senior view on conflicts and political tensions by positioning these situations in the frame of enterprise risk management, and Markus Müller-Fehrenbach, CISO Vetropack, together with Onysiia Kutsovol, subject-matter expert, will show what it means for ICT infrastructure to be attacked in war and what we should prepare for these situations. Finally, a framework for war readiness is presented – a valuable forward-thinking input

As usual, after each keynote presentation, we will run a discussion round:

- Discussion Round 1: Enterprise Risk Management in times of political conflicts: What has changed, and which additional use cases are important?
- Discussion Round 2: Making ICT operations more war-resilient: what is needed?

KEYNOTE I AND ROUNDTABLE I

3

Keynote I:
Enterprise Security Risk Management (ESRM): A Converged Approach to Security Governance

Since the end of the Cold War, resurgent geopolitical fault lines — Eastern Europe, the Middle East, the Taiwan Strait, the Indo-Pacific — are pressuring enterprises, supply chains, and critical infrastructure. Regulators are catching up: DORA, NIS2, and the EU Cyber Resilience Act signal hardening statutory duty-of-care obligations.

Doron Zimmermann argues traditional siloed security — IT security dominant, cyber security secondary, physical and personnel security lagging — is no longer adequate. Each silo gap is a self-inflicted attack surface. Without structured risk dialogue among key stakeholders (CISO Office, ERM, HR, Legal, Audit, Procurement, Corporate Security, Business Units, IT), individual gaps become an enterprise-wide vulnerability.

ESRM offers a converged, risk-principle-led alternative, anchored in the ESRM Cycle: Identify, Analyze & Assess, Treat & Mitigate, Monitor & Review, Stakeholder Dialogue. It treats security as integrated governance aligned to enterprise risk and objectives. Its Value Chain operationalizes this via five domains — Threatscape analysis, Value at Risk identification, Maturity & Resilience assessment, Countermeasures, and Program management — each answering a distinct strategic question.

Tailored to organizational maturity and supported by relevant standards (NIST CSF, ISO 27001, ASIS ESRM, GDPR, DORA), ESRM is delivered via modular or end-to-end engagement models.

Dr. Doron Zimmermann, Principal, Security Risk Management, EPAM EMEA Security Practice. 15+ years in cyber, information, and corporate security, including national security experience at cabinet level. I coach CSOs and CISOs on enterprise, cyber, and information security, drawing on a track record with executive teams and boards.

Core competencies: corporate security management, strategic security design, crisis and emergency management, threat intelligence, risk analysis, role-based security awareness training, and applying counter-intelligence methods to commercial contexts.

I help security functions across industries align policies, strategies, and controls across all lines of defense – delivering sustainable, targeted security while building a culture of awareness and resilience.

Discussion Round I:
Enterprise Risk Management in times of political conflicts: What has changed, and which additional use cases are important?

KEYNOTE IIA AND ROUNDTABLE II

4

Keynote II:
A production camp in Ukraine – preparation, incidents, lessons identified

Normal operation with framework- and compliance-oriented security is excellent for peacetime – but when war crosses the production camp, everything is different. Experience sharing from a real case in East Ukraine will position regular top security and provide a clear view of what we do not cover in our mainstream security thinking when war hits production camps.

The pictures of the devastating actions of soldiers give a clear understanding that war is completely beyond our imagination and that actions of preparation must be beyond what the security community has developed in standards, frameworks, and compliance requests.

Markus Müller-Fehrenbach, CISO at Vetropack, has more than 25 years of international leadership experience in IT and Information Security, covering IT strategy, infrastructure and operations, process optimization and transformation in international and multi-site organizations.

As an Information Security specialist with a strong technical background, he has expertise in ISO 27001-based Security Governance, security architecture, security and maturity assessments, and security roadmaps. His work focuses on assessing security capabilities, identifying gaps, and defining target states for improvement, considering business processes and capabilities as well as Data Protection and regulatory requirements. His knowledge of legal matters complements his technical and management experience. He advises executive management and IT leaders on cyber risks and sustainable security strategies.

A key part of his work is assessing existing security capabilities, identifying gaps and defining target states and realistic roadmaps for improvement. Business processes and business capabilities are an important part of this perspective, ensuring that security priorities and investments reflect actual business needs.

KEYNOTE IIB AND ROUNDTABLE II

4

Keynote II:
Cyber Defense of Critical Infrastructure Under Armed Conflict:
Lessons from the Russian–Ukrainian War

Modern critical infrastructure faces unprecedented cyber threats in conflict zones, where adversaries combine sophisticated APT operations with kinetic warfare. This talk presents findings from a master's thesis research project examining how Ukrainian critical infrastructure has been targeted by Russian state-sponsored threat actors – and what lessons other sectors and nations can draw from this experience.

Drawing on three major case studies (NotPetya, SolarWinds, and the Viasat/KA-SAT attack) and expert interviews, the presentation introduces the Cyber Shield Framework – a five-layer diagnostic model addressing the failure modes that emerge under wartime conditions. Key findings include how governance gaps, ZTA-monitoring coupling failures, and compressed decision-making cycles degrade cyber defenses precisely when they are needed most. The talk will offer practical recommendations for security professionals and policymakers responsible for protecting critical systems in high-pressure environments.

Onysiia Kutsovol has not long ago defended her Master thesis in Information Security at NTNU (Norwegian University of Science and Technology), where she completed her thesis on the protection of critical infrastructure against Russian APT threats. She holds a Bachelor's degree in Cybersecurity from the National Technical University of Ukraine. Alongside her studies, she works as a Student Assistant at NTNU, mentoring a peer in Network Security and Cyber Crime Investigation, and holds a bookkeeping role in the IT student association LOGIN. She previously worked as an IT Consultant at Hunton Fiber AS, where she managed access control, system administration, and risk planning using Microsoft 365 and Active Directory. Her technical expertise spans network security, ethical hacking, digital forensics, SIEM, and tools such as Wireshark, Metasploit, Nessus, and Palo Alto Networks.

Discussion Round II:
Making ICT operation war resilient: what is needed?

5 Information

What is the Swiss CISO Summit?

The Swiss CISO Summit facilitates the exchange of current security challenges and opportunities between security executives, managers, and thought leaders in Switzerland. Each summit addresses a current hot topic. The strategic dialog and the subsequent discussions are inspired by a keynote speech from well-recognised national and international speakers. The moderated and guided discussions in groups of 8–10 members share views, experiences and strategies. An excerpt of the discussions will be written down in the result paper for the participants.

Participation is by invitation only.

How does the Swiss CISO Summit maintain confidentiality?

The Swiss CISO Summit is provided as a closed-door event (please contact Bernhard Hämmerli for participation). This exclusive CISO Executive programme is created for information security and risk executives providing them with an environment for achieving new ways of thinking and ensuring success in protecting their organisations.

The summits are held strictly under the Chatham House Rules, under which shared information is treated with full discretion and kept confidential from people outside the group.

Why should I join the Swiss CISO Summit?

The Swiss CISO Summit has a unique concept of creating trusted circles amongst executives, managers and thought leaders. Meeting peers in a professional business setting, having time to network with each other, and discussing current issues create unique opportunities for sharing experiences and receiving advice beyond the discussion at the table.

- Extensive networking opportunities with peers and experts on an ongoing basis
- Meet with other leading executives to share successes, failures, obstacles, and challenges
- Learn about current strategies for managing security threats and preparing for the future
- Make new connections and equip yourself with information on recent projects and achievements

What makes the difference?

The Swiss CISO Summit has many and diverse benefits for the invited experts. The participants are the focal point of the summit and the meeting is not intended for providers to present solutions or products. Sales activities are strictly prohibited to preserve an open and candid exchange among CISOs.

What is the history behind the Swiss CISO Summit?

The Swiss CISO Summit has been run successfully since 2001 under the name «Risk and Security Exchange» and from 2004 - 2009 when it was known as „Swiss Security Exchange“. Then with the financial turmoil the summit came to a halt. From 2009 onwards, the same successful format was adopted in Norway where it ran under the name „Sikkerhetstoppmøte“. All this experience gained by Prof. Dr. Hämmerli is put into the organisation of the Swiss CISO Summit.

Information

5

Who prepares and facilitates the Swiss CISO summit?

An organising committee under the lead of Prof. Dr. Bernhard M. Hämmerli is responsible for the invitation, preparation and guidance of the discussions. He is an internationally well recognised expert with 25 years of experience in information security in governments, industry and academia. He led the Cyber Security activities of the Swiss Academy of Engineering Sciences SATW from 2012 – 2017.

Prof. Dr. Hämmerli is a founding member of the Information Security Society Switzerland and he built up the first Information Security master programme in Lucerne in 1996, respectively 1999, and since 2017 he is head of the new BSc Information & Cyber Security at Hochschule Luzern/Informatik. Additionally, he teaches at the Norwegian University of Science and Technology Norway www.ntnu.no, in the technology and management track of the Information Security master programme.

Prof. Dr. Hämmerli is supported by Katarzyna Kuhn for administrative purposes.

Agenda (generalised)

12:00	Start with a small lunch
12:45	Networking Session
13:15	Welcome and introduction
13:30	Keynote from experts or members
14:00	Roundtable session I
15:00	Exchange between the groups and wrap-up of roundtable I
15:10	Break
15:40	Keynote from experts or members
16:10	Roundtable session II
17:05	Exchange between the groups and wrap-up of Roundtable II
17:15	Summary note
17:30	Cocktail and aperitif
19:00	Closing

The meeting is held three times per year.

6 Registration

Join Swiss CISO Summit

Participation is by invitation only. We accept proposals for new participants. The number of participants is limited to 40 per summit in order to maintain an atmosphere of trustful information sharing.

Single summit CHF 450.- per participant
Three summits CHF 1'000.- per participant (25 % discount for booking three consecutive summits – not three participants at one summit)

Cancellation Policy

Cancellations of registrations are free of charge only if received no later than seven days before the summit. Cancellations received beyond this point will incur 100 % of the admission fee. In any case a delegate may be sent at no additional cost. More information is found at www.ciso-summit.ch. Content responsibility for the summits lies with Prof. Dr. Bernhard M. Hämmerli.

Register by just replying to the invitation email with all your details or by following these steps:
Step 1: Fill out & save the form
Step 2: Select Send button > email opens (info@ciso-summit.ch)
Step 3: Attach the PDF file

Registration PRINT RESET SEND

Register by just replying to the invitation email with all your details – or by filling out this form and mailing it to info@ciso-summit.ch

☐ **Three consecutive summits for CHF 1'000.—**
3 Summits 38 (Thursday 17.09.2026), 39 (Tuesday 26.01.2027), and 40 (Tuesday May 11, 2027)

☐ **38th Swiss CISO Summit**
17.09.2026: CHF 450.– for all forms of participation

First Name _____ Surname _____

Organisation _____

Street / No. _____ ZIP / City _____

Phone _____ Email _____

Signature _____ *Date* _____

Sponsorships & Partner 7

Platinum Sponsor	**Detecon**

Detecon Consulting is one of the world's leading management consulting companies for integrated management and technology consultancy. Detecon (Schweiz) AG is located in Zurich and bundles Financial Management as well as ICT Management competences among its roughly 150 employees. The main focus lies on the requirements of CFOs and CIOs in nearly all industry sectors. Globally, more than 6000 projects have been implemented successfully. The international spirit and the openness are reflected not only in the number and origin of our clients from over 160 countries but also in our employees that are recruited from 30 different nations.

Gold Sponsor	**PricewaterhouseCoopers**

At PwC, our purpose is to build trust in society and solve important problems. PwC looks at cyber security as one of today's biggest challenges and provides a full stack of cyber security consulting services. PwC's Cyber security practice comprises deep information security, forensic technology, business and technology resilience, Cybercrime response, technology risk and controls, project and program management and operations specialists to help clients address Cyber risks through the whole lifecycle from strategy to execution and operations.

Silver Sponsor	**Armed Forces Command Support Organisation (AFCSO) Cyber Command**

With its services in ICT and electronic operations, the Armed Forces Command Support Organisation (AFCSO) ensures that the armed forces can accomplish their missions. It guarantees the command and control of the armed forces under all conditions.

Silver Sponsor	**SWISS POST**

Swiss Post is part of the critical infrastructure of Switzerland. On top of its logistics and transport services, Swiss Post offers a variety of digitalized services in other industries, including electronic voting, eHealth and secure email. The ICT department holds certificates on ISO 27001, 22031 and 20000. Information Security is an integral part of all activities of Swiss Post Group. As a first mover in the Paris Call for Security and Trust in Cyberspace, Swiss Post Group fosters expertise sharing on security in trusted environments both nationally and internationally.

7 Sponsorships & Partner

Silver Sponsor	**HSLU**

Lucerne University of Applied Sciences and Arts
HOCHSCHULE LUZERN

Lucerne School of Computer Science and Information Technology provides the most comprehensive range of IT study programs within Switzerland. The Lucerne School of Computer Science and Information Technology offers bachelor's and master's degree programs, applied research and development, and continuing education programs in Computer Science, Information Technology and Business Information Technology. Innovative study programs developed over the past five years include: Information & Cyber Security, Artificial Intelligence and Machine Learning, Digital Ideation, and International IT Management.

Partner	**SATW**

satw it's all about technology

SATW is recognized as the Swiss organization for the communication of independent, objective, and comprehensive information about trends in technology – as a basis for the forming of well-founded opinions – and as an effective institution for the promotion of engineering sciences and new technologies in Switzerland. SATW identifies technological developments of relevance to industry and informs politicians and society about the significance and consequences of such developments.

swissciso summit

More information is found at www.ciso-summit.ch

Sponsorships:

Platinum

Gold

Silver

Partner: