Tallinn
Cyber Diplomacy
Winter School
2026

Agenda[1]

Tallinn Cyber Diplomacy Winter School 2026!

The **Tallinn Cyber Diplomacy Winter School** is designed to further develop the expertise of the Tallinn Summer School **Alumni** network and provide opportunities for discussing practical ways to strengthen cross-regional cooperation. The 3-day gathering, taking place from 2 to 4 March 2026 in Bangkok, Thailand, will enable alumni to deepen their professional connections, exchange regional insights, and address pressing cyber diplomacy and cybersecurity challenges through focused discussions, expert-led sessions, and collaborative activities.

Each Winter School focuses on different region-specific priorities, with input from the Alumni shaping the agenda to ensure relevance and practical impact. The 2026 edition will take place in Asia, and therefore, regional priorities and challenges will be highlighted throughout the agenda. However, such regional dimension will also provide an opportunity for participants from all regions to share their experiences and learn from each other. By fostering dialogue, sharing expertise, and promoting EU values, the Winter School aims to advance a free, open, secure, and resilient cyberspace globally.

Co-organised by the e-Governance Academy, the Estonian Ministry of Foreign Affairs, the National Cyber Security Agency Thailand National and the European Commission, the Winter School continues to grow a global community committed to a secure, stable and cooperative digital future.

[1] The organisers reserve the right to adjust the draft agenda and venues, ensuring the program's focus and goals remain unchanged.

Sunday, 1 March — Icebreaker at 19:00-21:30

Location: Royal Orchid Sheraton Riverside Hotel, Bangkok, Siam Yacht Club

Monday, 2 March — Keeping pace with evolving cyber threats: *How can we build a whole-of-society approach to cybersecurity in today's digital world?*

Location: Royal Orchid Sheraton Riverside Hotel Bangkok, Ballroom 2

Theme: The threat landscape is evolving rapidly and puts significant pressure on the governance and operational capacities of states, businesses, and citizens. Even if not all countries and regions face the same challenges or to the same degree, the global nature of phenomena such as ransomware, online scams, and attacks on critical infrastructure necessitates strengthening situational awareness and understanding of cybersecurity trends worldwide. **This day will focus** on regional perspectives, highlighting key trends and challenges as well as lessons and good practices from cybersecurity governance and collaboration.

The agenda will examine the evolving threat landscape from multiple angles, including both national and private sector perspectives. It will offer case studies and examine how emerging technologies, such as AI, reshape the cyber domain. Participants will share insights into effective governance models, discussing successes, challenges, and areas of convergence while fostering multistakeholder collaboration to counter cyber threats.

Moderator of the day: **Taimar Peterkop**, Senior Cybersecurity Expert, e-Governance Academy

<table>
<tr><th colspan="2">Morning session | 9:00-13:00 | Royal Orchid Sheraton Riverside Hotel Bangkok</th></tr>
<tr><td>8:30-9:30</td><td>Registration</td></tr>
<tr><td>9:00-9:30</td><td><b>Opening remarks</b>
<b>Ms Sara Rezoagli</b>, Chargée d'Affaires, Deputy Head of the European Union Delegation to the Kingdom of Thailand
<b>Air Vice Marshal (AVM) Amorn Chomchoey</b>, Secretary-General, National Cyber Security Agency (NCSA), Kingdom of Thailand
<b>Ms Helen Popp,</b> Ambassador-at-Large for Cyber Diplomacy, Ministry of Foreign Affairs of the Republic of Estonia
<b>Mr Hannes Astok,</b> Executive Director and Chairman of the Management Board, e-Governance Academy, Estonia</td></tr>
<tr><td>9:30-10:00</td><td><b>Scene-setting: The impact of critical technologies on cyber security domain</b>
<b>Benjamin Ang,</b> Head, Digital Impact Research, Singapore</td></tr>
<tr><td>10:00-10:45</td><td><b>Connectivity, cybersecurity and AI: threats and trends</b>
This session provides a strategic overview of the evolving cyber threat landscape, with a particular focus on regional dynamics and the growing</td></tr>
</table>

	influence of artificial intelligence. It combines a global threat picture with concrete case studies and lessons learned from recent incidents, especially those impacting the connectivity infrastructure. The session also explores how AI is reshaping offensive and defensive cyber capabilities, creating new challenges for detection, attribution, and response, while raising policy and governance implications for states and institutions. Learning objectives: ✖ Understand current global and regional cyber threat trends and their strategic implications, especially the impact on secure connectivity and the investment environment. ✖ Assess how artificial intelligence is transforming the cyber threat landscape and national response capabilities. Speakers: ✖ **Kimmo Rousku**, General Secretary of the Public Sector Digital Security Management Board (VAHTI), Senior Expert at the Finnish Digital Agency, Finland
10:45-11:15	Coffee break
11:15-13:00	**Deep dives into specific threats: Technical, diplomatic and criminal justice responses** This session offers an in-depth examination of selected high-impact cyber threats and the multi-layered responses they require in order to promote resilience and an environment conducive to investment. Focusing on attacks against critical infrastructure, ransomware campaigns, online scams, and the spread of illegal content, speakers will analyse how these threats manifest in practice and evolve across borders. They will also look at the role that trusted providers play in strengthening country's preparedness and response capabilities. The session brings together technical perspectives on prevention, detection, and incident response with diplomatic tools, as well as criminal justice approaches including investigation, evidence-sharing, and prosecution. Emphasis is placed on coordination across communities to ensure coherent and effective responses. Learning objectives: ✖ Identify the technical, legal, and diplomatic dimensions of major contemporary cyber threats. ✖ Understand how cross-border cooperation enhances prevention, response, and accountability. Speakers: ✖ **Andrii Davydiuk**, Head of Branch, NATO CCDCOE, Ukraine, *alumni of Tallinn Cyber Diplomacy Summer School* ✖ **Yukako Uchida**, JPCERT/CC Global Coordination Division, Japan

	Arthur Langellier, Cybercrime Strategy Officer, INTERPOL **Angelica Cusmà Lorenzo**, Cybersecurity Strategic Advisor at Leonardo Cyber & Security Division
13:00-14:00	Lunch
Afternoon session | 14:00-15:15 | Royal Orchid Sheraton Riverside Hotel Bangkok	
14:00-15:15	**Strengthening whole-of-society approach to cyber governance** This session explores how states can build resilient and inclusive cyber governance frameworks through a whole-of-society approach, especially including the role of the private sector. Drawing on practical experiences from developing national cybersecurity ecosystems—including emerging AI ecosystems—speakers will discuss strategy formulation, institutional role allocation, and policies that enable domestic capabilities and innovation. The session examines cooperation models for public—private partnerships, highlighting how trust, information sharing, and shared responsibility can be operationalised. It also distils lessons from multistakeholder engagement, with a focus on aligning security objectives with economic development, innovation, and societal resilience. Learning objectives: Understand how to design and implement a whole-of-society approach to national cyber governance. Analyse effective models for public—private and multistakeholder cooperation in cybersecurity and AI. Speakers: **Prof Dr Ida Madieha Bt. Abdul Ghani Azmi**, International Islamic University Malaysia **Jakob Piaskowski**, Head of Office for Structuring and Management of Financial Instruments, Department for International Development Instruments, BGK (Bank Gospodarstwa Krajowego), Poland **Liina Areng**, Project director, EU CyberNet, Estonia **Atul Kumar,** Director, Data Security Council of India, alumni of Tallinn Cyber Diplomacy Summer School
15:15	Family photo
15:30-15:45	Coffee break
Table-Top Exercise part 1 | 15:45-17:00 | Royal Orchid Sheraton Riverside Hotel Bangkok	
	Moderator: **Patryk Pawlak,** Part-time Professor, Robert Schuman Centre for Advanced Studies, European University Institute The scenario-based discussions will translate knowledge into practice through an interactive workshop. Participants will examine cross-border digital dependencies in an interconnected region, identify critical interdependencies,

	assess their impact on national and regional resilience, and explore cooperation models to address them. Through practical discussions, participants will develop actionable approaches relevant to their national contexts and strengthen their ability to contribute to cybersecurity strategies and regional dialogue. Participants will receive background materials and the scenario in advance. Goals of Part 1: ✖ Identifying key issues and challenges ✖ Designing national responses at the policy, technical and operational levels **Locations and Facilitators:** **Group 1**: Elina Noor - Ballroom 3 **Group 2**: Liina Areng - Ballroom 3 **Group 3**: Helen Popp - Riverside 1 **Group 4:** Pavel Mraz - Riverside 2
Evening programme I 18:00 — 22:00 I	
18:00	Gathering in the hotel lobby. The transfer will take approximately 40—50 minutes by van. Networking event and dinner at the restaurant **Supatra River House** (Address: 266 Soi Wat Rakhang, Arun Amarin Road, Siriraj, Bangkok Noi, Bangkok)

Tuesday, 3 March — How to link global norms and national implementation effectively?

Theme: National legislative and institutional frameworks are the foundation of cyber-resilient nations. However, even the most advanced countries cannot manage and respond to cyber threats alone, whether cybercrime or malicious activities driven by states or their proxies. This day will focus on providing a comprehensive overview of the state of play regarding the UN framework of responsible state behaviour and provide a forward-looking analysis ahead of the launch of the new UN Global Mechanism in March 2026. It will explore how to preserve the progress achieved by the international community and address the outstanding controversies. Discussions will highlight recent developments in the international framework of responsible state behaviour in cyberspace, their implications for local contexts, and ways to better integrate these advancements at national and regional levels.

Moderator of the day: **Patryk Pawlak,** Part-time Professor, European University Institute; Visiting scholar, Carnegie Europe

<table>
<tr><th colspan="2">Morning session | 9:00-13:00 | Royal Orchid Sheraton Riverside Hotel Bangkok</th></tr>
<tr><td>9:00-9:30</td><td><b>Scene-setting: Geopolitics of critical technology: the role of international cooperation in managing cyber threats associated to new technologies</b>
- <b>Dr Tobias Feakin,</b> Managing Director Protostar Strategy, Former Ambassador for Cyber affairs and Critical Technology of Australia</td></tr>
<tr><td>9:30-10:45</td><td><b>The achievements and the future of the UN framework of responsible state behaviour</b>
This session examines the achievements and future prospects of the UN framework of responsible state behaviour in cyberspace. It reviews key normative outcomes, including agreed norms, confidence-building measures, international law, and assesses how these have been implemented at national and regional levels. Speakers will reflect on practical experiences from cyber diplomacy, highlighting both successes and persistent challenges such as compliance, attribution, and accountability. The session also looks ahead to emerging issues—such as AI-enabled cyber operations—and discusses how the framework may adapt to remain relevant and effective in a changing technological and geopolitical environment.
Learning objectives:
- Understand the core elements of the UN framework of responsible state behaviour in cyberspace.
- Assess future challenges and opportunities for strengthening its development, implementation and relevance.
Speakers:
- <b>Pavel Mraz</b>, APAC Capacity-Building, Cybersecurity Researcher, United Nations Institute for Disarmament Research (UNIDIR)</td></tr>
</table>

	✖ **Julia Rodriguez**, Minister Counsellor, Cybersecurity Expert, Permanent Mission of El Salvador to the United Nations, El Salvador, *alumni of Tallinn Cyber Diplomacy Summer School* ✖ **Kubo Mačák**, Professor of International Law, University of Exeter, UK
10:45-11:00	Coffee break
11:00-12:00	**Group discussion: From global norms to national implementation** This interactive session aims to bridge the UN framework of responsible state behaviour with national and regional contexts. It seeks to explore how developments at the UN are aligned at the national and regional levels, identify practical ways to enhance the integration of the UN framework, and frame the discussion around leveraging the process for tangible national and regional benefits. **Structure**: Participants will be divided into groups to foster practical discussions on leveraging global and regional processes (including at the UN and within regional organisations) to address local needs and challenges. Discussions will focus on: ✖ Exchanging information about key cyber threat and risks ✖ Approaches and methods to address attacks on critical infrastructure, ransomware, scams and illegal content online. ✖ Ongoing regional processes to deal with these challenges Participants will be asked to reflect on the current developments in participants' countries and/or regions and discuss how the local or regional challenges can be better addressed through international cooperation. The aim is to allow for the exchange of insights on best practices, identifying common challenges, and exploring actionable solutions within national and/or regional contexts.
12:00-12:30	Recap session **Findings and results from the group discussions** Each group presents their findings and discussion outcomes, with the focus on aligning international commitments with national and/or regional processes.
12:30-13:30	Lunch
Afternoon session | 13:30-15:30 | Royal Orchid Sheraton Riverside Hotel Bangkok	
13:30-14:30	**Accountability and diplomatic responses to malicious cyber activities** This session focuses on recent cases of how states and international actors pursue accountability for malicious cyber activities through diplomatic, legal, and normative tools. It examines the range of diplomatic responses available, including attribution statements, demarches, sanctions, and collective responses coordinated through regional and international organisations. Speakers will discuss the political and evidentiary challenges of attribution, the role of international law, and the interaction between national decision-making and multilateral processes. The session also explores how accountability

	mechanisms can contribute to deterrence, stability, and the reinforcement of responsible state behaviour in cyberspace, while managing escalation risks. Learning objectives: - Understand the spectrum of diplomatic and accountability tools available in response to malicious cyber activities. - Analyse the challenges of attribution and their implications for effective and responsible cyber diplomacy. Speakers: - **Helen Popp**, Ambassador-at-large for cyber issues, Ministry of Foreign Affairs of Estonia - **Noriko Tanaka,** Deputy Director, National Security Policy Division Ministry of Foreign Affairs, Japan, *alumni of Tallinn Cyber Diplomacy Summer School* - **Mahé Dersoir**, Deputy Director of Cybersecurity, Ministry for Europe and Foreign Affairs, France - **Claudio Peguero**, Ambassador for Cyber affairs, Ministry of Foreign Affairs, Dominican Republic, *alumni of Tallinn Cyber Diplomacy Summer School*
14:30-15:30	**Cyber capacity building before and after the UN Global Mechanism** This session examines the evolution of cyber capacity building and its future in light of the establishment of the UN Global Mechanism. It reviews key goals and ambitions of international capacity-building efforts, highlighting shifts in priorities, and coordination. Speakers will explore practical ways to strengthen cooperation with an emphasis on how national interests and priorities increasingly redefine key principles of needs-driven approaches, sustainability, and local ownership. In that context, they will make the case for the need to shift the logic of cyber capacity building from being driven by development narrative to the investment imperative. Learning objectives: - Understand how the UN Global Mechanism reshapes the landscape of cyber capacity building. - Identify good practices for effective cooperation between donors and partner countries. Speakers: - **Andrea Leone**, Team Leader, Digital Transformation Unit, Directorate General for International Partnerships, European Commission - **Kerry-Ann Barrett**, Chief of Cybersecurity Section, Inter-American Committee against Terrorism (CICTE), OAS - **Tupou'tuah Baravilala**, Director-General Digital Government Transformation, Cybersecurity and Communications Ministry of Policing and Communications Suva, Fiji
15:30-16:00	Coffee break

<table>
<tr><th colspan="2">Table-Top Exercise part 2 | 16:00-17:30 | Royal Orchid Sheraton Riverside Hotel Bangkok</th></tr>
<tr><td></td><td>Group discussion continues with new injects. Goals of the exercise:
✖ Explore opportunities for international and cross-regional cooperation
✖ Discuss diplomatic responses to a cyber incident
<b>Locations and Facilitators:</b>
<b>Group 1</b>: Elina Noor - Ballroom 3
<b>Group 2</b>: Liina Areng - Ballroom 3
<b>Group 3</b>: Helen Popp - Riverside 1
<b>Group 4:</b> Pavel Mraz - Riverside 2</td></tr>
<tr><th colspan="2">Evening programme I 18:30 — 22:00 I</th></tr>
<tr><td>18:30</td><td>Gathering in the hotel lobby and walking to the River City Building, Gate 2 (dinner and evening programme)
<b>Networking event at Wonderful Pearl Cruise (Dinner on Cruise)</b></td></tr>
</table>

Wednesday, 4 March — Regional and cross-regional cooperation: We are in it together, now what?

Theme: Regional cooperation frameworks are an important complement and facilitator between the national and global levels. They assist their members in gaining a deeper understanding of the complex global cyber issues and support them in translating their international commitments into local action. They offer the necessary support to contextualise global debates at the national level and help global audiences understand local conditions. But not all regional organisations have similar mandates, resources and tools. Understanding how they can support each other and learn to best support their members is critical. The final day will be devoted to exploring how different regional organisations can be more effective and work together better. In that sense, the focus will be on addressing regional cross-border (inter)dependencies in cooperation and collaboration.

Moderator of the day: **Elina Noor**, Non-resident Scholar, Asia Program, Carnegie Endowment for International Peace

Morning session | 9:00-12:30 | Royal Orchid Sheraton Riverside Hotel Bangkok	
9:00-9:30	**Scene-setting: Enhancing Cooperation with the Multistakeholder Community** ✖ **Julien Sylvestre-Fleury**, Senior Policy Advisor, Global Affairs Canada, *alumni of Tallinn Cyber Diplomacy Summer School*
9:30-10:45	**Role of regional organisations in strengthening cyber resilience and responsible state behaviour in cyberspace** This session explores the role of regional organisations, while also identifying gaps and opportunities for stronger cross-regional cooperation. It examines regional approaches to norm implementation, confidence-building measures, capacity building, and incident response cooperation. Speakers will discuss how regional organisations can bridge global frameworks and national implementation by adapting norms and policies to specific political, legal, and threat contexts. Particular attention is given to existing coordination gaps, fragmentation across regions, and opportunities for improved cross-regional cooperation in promoting secure connectivity and derisking investments in the digital domain. Learning objectives: ✖ Understand the functions and comparative advantages of regional organisations in cyber governance. ✖ Identify gaps and opportunities for strengthening cross-regional cooperation on cyber resilience and norms implementation. Speakers: ✖ **Kerry Ann Barrett**, Chief of Cybersecurity Section, Inter-American Committee against Terrorism (CICTE), Organisation of American States (OAS) ✖ **Camille Lalevée**, Policy Officer, Digital Transformation Unit, Directorate General for International Partnerships, European Commission

	- **Dr Gatra Priyandita**, Senior Analyst, Cyber, Technology and Security Program, Australian Strategic Policy Institute's (ASPI) - **Rachida Mamade**, Senior Cybersecurity Officer, Department of Political Affairs Peace and Security, African Union Commission, *alumni of Tallinn Cyber Diplomacy Summer School*
10:45-11:10	Coffee break
Table-Top Exercise part 3 | 11:15-13:15 | Royal Orchid Sheraton Riverside Hotel Bangkok	
11:15-13:15	Final injects and preparation of the group presentations **Locations and facilitators:** **Group 1**: Elina Noor - Ballroom 3 **Group 2**: Liina Areng - Ballroom 3 **Group 3**: Helen Popp - Riverside 1 **Group 4:** Pavel Mraz - Riverside 2 **Group presentations, feedback and discussion — Ballroom 3**
13:15-13:30	Closing remarks
13:30-14:30	**Lunch**