Tallinn Cyber Diplomacy Summer School 2024!

In 2024, the rapidly evolving digital landscape has further cemented the significance of cyber diplomacy in international relations. Cybersecurity and digitalisation are pivotal in diplomatic discussions, addressing challenges such as state-sponsored cyber operations, cybercrime, and the strategic impacts of emerging technologies like AI. The need for cohesive international collaboration and governance has never been more critical.

Participants are invited to join discussions at the intersection of foreign policy and technology, and to explore the cyber policies and practices of regional and international organisations.

Topics and Agenda

Day 0 (10 November) — Icebreaker at POCO in Rotermann City
19:00 — 21:30

Day 1 (11 November) — Digital and Cybersecurity Foundations. The Evolution of Emerging Technologies (AI).
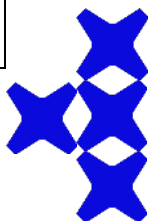
Theme: The first day of the course will establish the context for the work of a cyber diplomat by covering the fundamentals of cybersecurity — not as an end in itself, but as an enabler for a functional digital society that benefits its people and economy. Why do states engage in digitalisation and why does cybersecurity matter? What are the key threats and vulnerabilities, who are the threat actors, and how is cyberspace defended? What is the strategic impact of emerging technologies like AI? Discussions will provide participants with a comprehensive understanding of how digital technologies impact cybersecurity practices and policy development, laying the foundation for further exploration into cyber diplomacy.

Moderator of the day: **Tanel Sepp**, *Ambassador-at-Large for Cyber Diplomacy, Ministry of Foreign Affairs of Estonia*

Morning session	9:00-14:00	Hotel Nordic Forum	
9:00-9:30	Registration and gathering
9:30-10:15	Opening remarks **Burhan Gafoor**, Ambassador and Permanent Representative of Singapore to the United Nations in New, (online) **Minna-Liina Lind**, Undersecretary for Global Affairs, Ministry of Foreign Affairs of Estonia **Ariane Labat**, Head of Unit F5, Digital Transformation at the Directorate-General for International Partnerships of the European Commission **Hannes Astok**, Executive Director and Chairman of the Management Board, e-Governance Academy

10:15-11:00	The case for digitalisation as an enabler Why does digitalisation matter, why does cybersecurity matter to digitalisation? **Rain Ottis**, Professor of Cyber Operations at TalTech — Tallinn University of Technology **Dan Bogdanov**, Chief Scientific Officer at Cybernetica, Member of the Estonian Academy of Science
11:00-11:30	Coffee break & networking
11:30-12:00	The technology of geopolitics **Luukas Kristjan Ilves**, Former government CIO, Estonia
12:00-12:45	National cyber threat landscape. Vulnerabilities and threats, actors and risks. **Märt Hiietamm**, Head of Analysis and Prevention Department of Information System Authority of Estonia (RIA) **Peeter Marvet**, NCP C3, analyst of National Criminal Police, Estonian Police and Border Guard Board
12:45-14:15	Lunch
Afternoon session | 14:00-16:45 | Hotel Nordic Forum	
14:15-15:15	Global cyber threats and trends, role of AI in the threat landscape. Insights from global defenders in industry. **Paul Tumelty**, Mandiant Regional Leader UKI & Practice Leader EMEA Government of Google Cloud **Nikolas Ott**, Senior Manager of Government Affairs, Microsoft
15:15-15:45	Coffee break & networking
15:45-16:45	Disinformation How will AI change the game—benefits and risks. Experts delve into AI's role in disinformation, emphasizing its benefits and risks in the public sector and media **Jakub Janda**, Executive Director, European Values Center for Security Policy **Henrik Roonemaa**, Tech Journalist, Podcast Host, Producer of Delfi Meedia
Evening programme | 17:45-22:30 | Flower Pavilion (Lillepaviljon)	
17:45	Gathering at the Hotel lobby

18:00-21:30	Fireside chat session
	18:30 – 19:30 Kersti Kaljulaid, President of Estonia (2016-2021)
	Interviewed by Journalist and Foreign Editor **Indrek Lepik**
19:30	Dinner at Flower Pavilion (Lillepaviljon)
21:45	Transfer back to the Hotel

Day 2 (12 November) — Cyber Diplomacy and International Cybersecurity Frameworks
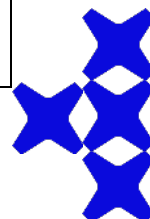
Theme: Day 2 focuses on the existing international cybersecurity and stability frameworks and mechanisms that govern state actions. The goal is to provide cyber diplomats with a comprehensive overview of the cyber diplomacy environment and key concepts they can engage with, enabling them to participate in international discussions in a productive and impactful manner. Sessions will look into norms of responsible state behaviour, international law governing state cyber activities, and confidence-building measures. A panel discussion with cyber ambassadors will help operationalise how diplomats navigate these frameworks and how they can enhance their effectiveness on international platforms.

*Moderator of the day: **Kerli Vesk**i, Under-Secretary of Legal and Consular Affairs, Ministry of Foreign Affairs of Estonia*

Morning session | 9:00-14:00 | Hotel Nordic Forum	
9:00-9:30	Keynote: The international cyber stability framework. The role for Cyber Diplomacy.
	Nathaniel Fick, Ambassador at Large, Cyberspace & Digital Policy. U.S. Department of State, (online)
	Tanel Sepp, Ambassador-at-Large for Cyber Diplomacy, Ministry of Foreign Affairs of Estonia
9:30-10:30	Norms of responsible state behaviour and cyber security confidence building measures.
	Katherine Priezman, Political Affairs Officer, United Nations Office for Disarmament Affairs, (online)

	Szilvia Tóth, Cyber Security Officer, Secretariat of the Organization for Security and Co-operation in Europe (OSCE) **Sithuraj Ponraj (CSA)**, Director, International Cyber Policy Office, Cyber Security Agency of Singapore **Mariana Jaramillo,** Cybersecurity Program Officer, Organization of American States (OAS)
10:30-11:00	Coffee break & networking
11:00-12:00	International law in cyberspace. International law applicable to state cyber activities in peacetime and conflict. **Dr. Przemysław Roguski**, Assistant Professor, Jagiellonian University in Kraków **Marguerite Walter,** Attorney-Adviser, Office of the Legal Adviser, U.S. Department of State
12:00	Blue Hoodie Day! Let' take the family photo
12:30-13:30	Lunch
Afternoon session | 13:30-15:15 |	
13:30-14:00	Implementing the cyber stability framework: the UN (in) action **Alban Andreu**, Policy Officer, Strategic Affairs and Cybersecurity Department, Ministry for Europe and Foreign Affairs of France
14:00-14:45	Protecting and promoting human rights online and offline **Rasmus Lumi**, Director General, Department of International Organisations and Human Rights, Ministry of Foreign Affairs of Estonia **Hille Hinsberg**, Open Governance Expert, Proud Engineers
14:45 -15:15	Brainstorming session: Estonia's next global digital and cyberspace policy **Luukas Kristjan Ilves**, Former government CIO, Estonia **Tanel Sepp**, Ambassador-at-Large for Cyber Diplomacy, Ministry of Foreign Affairs of Estonia
15:45-17.30	Gathering at the hotel lobby **Guided City Tours.** Explore the enchanting Old Town, featuring its medieval architecture, iconic landmarks, and rich history.
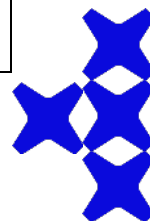
Evening programme	18:30-22:30	The Seaplane Harbour, Vesilennuki 6, Tallinn	
18:15	Gathering at the Hotel lobby, transfer
18:30	Fireside chat: How technology rules the world? Will technology dominate our future? Technology and the future. Opportunities and challenges of technology today and in the future. Dilemmas for national security and approaches to futureproofing. **19:00 – 20:00 Linnar Viik**, Information Technology Scientist, Entrepreneur, and Visionary in Digitalisation. Interviewed by **Hannes Astok**, Chairman of the Management Board, e-Governance Academy
20:00	Dinner at the Seaplane Harbour
22:00	Transfer back to the Hotel

Day 3 (13 November) — Cyber Diplomacy in Action: Possible Tools and Measures
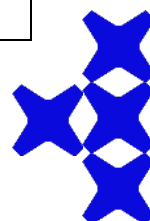
Theme: The third day will be dedicated to the implementation of cybersecurity frameworks, focusing on the implementation mechanisms for international law and cyber norms. The session will particularly look at the practical applications of state responsibility: what steps are needed to hold malicious actors accountable for their actions? How does attribution work in practice and what is the role of national cyber resilience? The goal is to help participants see how the existing cyber diplomacy tools and mechanisms can be applied effectively to prevent and manage cyber crises, and what architecture and processes are needed on the national level to operationalise the tools offered by the existing stability frameworks. The session will also introduce collective diplomatic and cyber defence frameworks of the EU and NATO.

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

Morning session	9:00-13:00	Hotel Nordic Forum	
9:00-9:30	State accountability, response and resilience. What are they and why are they needed?

	Heli Tiirmaa–Klaar, Chair of IT Coalition Steering Group, Ukraine Defence Contact Group. Visiting Distinguished Fellow, GMF Technology Programme
9:30–10.30	Mechanisms of state accountability. Case studies from the European Union and NATO. **Helen Popp**, Senior Expert, European External Action Service (EEAS) **Amy Ertan**, Cyber and Hybrid Policy Officer at NATO Headquarters
10:30–11:00	Coffee break & networking
11:00–12:00	State diplomatic responses to malicious cyber activity: legal, technical and political considerations – picking the suitable tools to respond. **Liesyl Franz**, Deputy Assistant Secretary for International Cyberspace Security in the U.S. Department of State's Bureau of Cyberspace and Digital Policy **Rupert Bailey,** Deputy Head, Cyber Threats, Foreign, Commonwealth and Development Office, United Kingdom **Shariffah R Syed Othamn**, Director of National Cyber Security Agency, National Security Council of Malaysia, (online)
12:00–13:00	Lunch
Afternoon session | 13:00-14:45 | Hotel Nordic Forum	
13:00–13:45	How to write a national position on the applicability of International Law in cyberspace. **Tereza Janakova**, Legal Officer at the International Law Department, Ministry of Foreign Affairs of the Czech Republic **Ágnes Kasper**, PhD, Head of Law Branch at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)
13:45–14:15	Building national resilience: what is national digital and cyber resilience ecosystem. Objectives, principles, and architecture of national cybersecurity from a national perspective. **Gert Auväärt**, Head of the Cyber Security Centre (NCSC-EE), Information System Authority of Estonia (RIA)
Side visits | 14:30 — 17.00 |	
14:30	Gathering at the Hotel lobby Transfer to the field visit in two groups

14:45-15:45 16:15-17:15	What is Cyber Defence League — the role of military cyber defence in national cybersecurity **Mihkel Tikk**, Deputy Commander, Estonian Defence Forces Cyber Command Location: Estonian Ministry of Foreign Affairs	Introduction of NATO CCDCOE activities **LtCol Bernard Hoffmann,** Deputy Director Chief of Staff Location: NATO Cooperative Cyber Defence Centre

Evening programme | Teras Beach | Tallinn Indoor Beach	
18:30	Gathering at the Hotel lobby Transfer to Tallinn Indoor Beach (Address Lõuka 6)
19:00	Dinner discussion: Cyber ambassadors' perspective. **Tupou'tuah Baravilala**, Director-General of Digital Government Transformation, Cybersecurity and Communications, Ministry of Trade, Co-Operatives, Micro, Small and Medium Enterprises, and Communications, Fiji **Claudio Peguero**, Ambassador, Advisor on Cyber-matters, Ministry of Foreign Affairs, Dominican Republic **Liesyl Franz**, Deputy Assistant Secretary for International Cyberspace Security in the U.S. Department of State's Bureau of Cyberspace and Digital Policy **Tanel Sepp**, Ambassador-at-Large for Cyber Diplomacy, Ministry of Foreign Affairs, Estonia
	It's time for a Beach Party! Let's dig our toes into warm sand, enjoy delicious snacks and refreshing drinks. Location: Teras Beach (Indoor beach)
23:00	Transfer back to the Hotel

Day 4 (14 November) — Building Cyber Resilience Through Diplomacy: Cyber Norms Implementation Providing a Vision for the Cyber Capacity Building
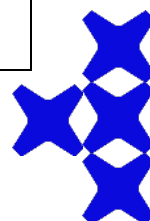
Theme: Building cyber resilience is a key aspect of maintaining and strengthening global and national security architectures. This day will offer practice-oriented insight on how to tap into cybersecurity capacity building initiatives to improve national cyber and regional cyber resilience, what are the interlinkages between cyber capacity building, national cyber resilience and implementation of international stability frameworks, and how cyber diplomacy relates to strengthening the national cyber resilience through capacity building. The aim is to equip participants with knowledge and skills to help them maximise the benefit of capacity building initiatives for their own countries.

***Merle Maigre**, Director of Cybersecurity Competence Centre, e-Governance Academy*

Morning session | 9:00-12:35 | Hotel Nordic Forum	
9:00-9:45	Contextualising capacity building - aspects, approaches and strategies. Understanding the links between cyber resilience, cyber capacity building and cyber stability frameworks. Incident response for policy makers **Hans de Vries**, Chief Cybersecurity and Operations Officer, European Union Agency for Cybersecurity (ENISA) **Merle Maigre**, Director of Cybersecurity Competence Centre, e-Governance Academy
9:45-10:45	Cybersecurity capacity building in practice: regional priorities, challenges, and lessons learned. Donor and implementer perspective. **Camille Lalevee**, Cybersecurity Policy Officer, Unit F5- Digital Transformation, Directorate General for International Partnerships, European Commission **Silja-Madli Ossip**, Community Lead for the EU CyberNet at the Estonian Information System Authority (RIA) **Cristina Camacho-Terán**, Minister of International Cooperation & Partnerships, Mission of Ecuador to the European Union, (online)
10:45-11:15	Coffee break & networking
11:15-12:15	Cybersecurity capacity building as a diplomatic priority in practice: Challenges, lessons learned and global and regional priorities: Beneficiary perspective.

	Selection from participants
12:15-12:35	National Cyber Security Index — u**nderstanding and leveraging the NCSI for maximum benefit**.
	PhD. **Radu Serrano,** Expert of Cybersecurity Competence Centre, E-Governance Academy
12:35-13:35	Lunch
14:00	Gathering at the Hotel lobby. Transfer to Vabamu Museum of Occupations and Freedom
Afternoon session | 14:30 — 17:00 | Vabamu Museum of Occupations and Freedom	
14:30-15:30	Case Study: Cyber Assistance to Ukraine — Tallinn Mechanism and IT-Coalition
	Hanna Postoliuk, Third Secretary of the Cyber Diplomacy Department, Minsitry of Foreign Affairs of Ukraine
	Andrii Davydiuk, Ukrainian representative and researcher at the NATO CCDCOE
	Laura Danilas, Head of Cyber Policy | NATO and European Union department, Ministry of Defence of Estonia
	Tanel Sepp, Ambassador-at-Large for Cyber Diplomacy, Ministry of Foreign Affairs of Estonia
15:30-16:00	Coffee break & networking
16:00-17:00	Case study: Story of Estonia´s reform through digitalisation and cybersecurity.
	Toomas Hendrik Ilves, President of Estonia (2006—2016), Visiting Professor of Tartu University
	Luukas Kristjan Ilves, Former Government CIO, Estonia
17:30	Transfer back to the Hotel
20:00	Free Evening
	For those interested, the dinner will be provided in the hotel.

Day 5 (15 November) — Practical Workshop. Exercise and Wrap-Up

Theme: The final day is dedicated to applying the knowledge and skills learned through a practical workshop/exercise, so they are equipped to not just understand but also actively engage in the formulation and execution of cybersecurity policies within their respective national contexts. The workshop aims to bridge theoretical knowledge with practical skills, preparing participants to make informed, strategic decisions in the realm of cyber diplomacy. This capacity ensures that they are well-equipped to handle real-world cyber challenges, influencing both the formulation of national positions and the international cybersecurity landscape.

The course concludes with a review of key insights and the handover of course diplomas.

Moderator of the day: **Tanel Sepp**, *Ambassador-at-Large for Cyber Diplomacy, Ministry of Foreign Affairs of Estonia*

Morning session	9:00-12:30	Hotel Nordic Forum	
09:00-12:30	Practical workshop
	Table-top exercise
	Including Coffee break & networking
	Lauri Almann, Exercise Moderator
	Aare Reintam, Cybersecurity Lead Expert
	Markus Ilmar Münzer, Exercise Technical Lead
12:30-13:30	Lunch
13:45	Gathering at the Hotel lobby. Transfer to the Maarjamäe Palace of Estonian History Museum.
Afternoon session	14:00-17:00	The Maarjamäe Palace of Estonian History Museum.	
14:15	Keynote speech
	Margus Tsahkna, Minister of Foreign Affairs

	Conclusions of the Tallinn Cyber Diplomacy Summer School **Tanel Sepp**, Ambassador-at-Large for Cyber Diplomacy, Ministry of Foreign Affairs of Estonia **Camille Lalevee**, Policy Officer for Cybersecurity, Science, Technology, Innovation and Digitalisation, European Commission (DG INTPA) **Hannes Astok**, Executive Director and Chairman of the Management Board, e-Governance Academy **Minna-Liina Lind,** Undersecretary for Global Affairs, Ministry of Foreign Affairs of Estonia
	Handover of diplomas
15:30 — 17:00	Networking reception
17:00	Transfer back to the Hotel

Contacts:

General inquiries:

cyberschool@mfa.ee

Organisational topics:

Ene Višnev, Project Manager of the EU Support for Tallinn Summer School of Cyber Diplomacy project; Senior expert of Cybersecurity Competence Center, e-Governance Academy, ene.visnev@ega.ee

Triinu Raigna, Training Expert, e-Governance Academy, +372 51 44 724, triinu.raigna@ega.ee