Tallinn
Cyber Diplomacy
Summer School
2025

16-20 June

Tallinn Cyber Diplomacy Summer School

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 global collaboration and governance has never been more critical.

The sixth edition of The Tallinn Cyber Diplomacy Summer School will explore these essential themes, providing a platform for diplomats, experts and policymakers to enhance their understanding, skills and role in navigating the complex cyber domain. Building on the success of previous years, this event continues to foster a secure, resilient, and open cyberspace.

Participants

This five-day event is designed for diplomats who have recently taken on the challenging task of cyber foreign policymaking, as well as other government officials and policy makers interested in complex cyber issues.

Lecturers

The Summer School will feature distinguished current and former cyber diplomats, policymakers, and experts from the private sector, academia, and civil society in the international arena.

Venue

The primary venue is the Hotel Nordic Forum, a modern four-star business and conference hotel in the heart of Tallinn, on the edge of the picturesque Tallinn Old Town, a UNESCO World Heritage site.

Contact

For further information, please contact tallinn@cyberdiplomacy.ee

Global Gateway

Republic of Estonia
Ministry of Foreign Affairs

eGA e-governance academy

estdev From the people of Estonia

Topics and Agenda

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.

Day 1

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? What are the current AI governance models and how do they address the benefits and risks of 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.

Day 2

Day 2 focuses on 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, confidence-building measures, and touch upon possible future mechanisms after the mandate of the OEWG. A panel discussion with cyber ambassadors will help operationalise how diplomats navigate these frameworks and how they can enhance their effectiveness on international platforms.

Day 3

The third day will be dedicated to implementing cybersecurity frameworks, focusing on the implementation mechanisms for international law and cyber norms. The session will mainly 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 the EU and NATO's collective diplomatic and cyber defence frameworks.

Day 4

This day will offer practice-oriented insight on how to tap into cybersecurity capacity-building initiatives to improve national and regional cyber resilience, the interlinkages between cyber capacity building, national cyber resilience, and the implementation of international stability frameworks, and how cyber diplomacy relates to strengthening 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.

Day 5

The final day is dedicated to applying the knowledge and skills learned through a practical workshop/exercise so that participants 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 cyber diplomacy. This capacity ensures that they are well-equipped to handle real-world cyber challenges, influencing the formulation of national positions and the international cybersecurity landscape.

Diverse learning formats

In addition to classroom lectures, panel discussions and workshops, the agenda features field visits to relevant cybersecurity and/or government entities. These visits provide practical insights into the operations and strategies employed in cybersecurity.

The program also includes a hands-on cybersecurity exercise, simulating realistic scenarios to enhance participants' practical skills and preparedness.

Social and networking programme

The Summer School's evening program includes an icebreaker reception, hosted dinners, fireside chats with inspirational speakers, guided tours, and numerous networking opportunities. These events are designed to foster connections among participants, encouraging the exchange of ideas and experiences in a relaxed and informal setting.

About the organisers

Directorate-General for International Partnerships (DG INTPA), is the European Commission's department responsible for formulating the EU's international partnership and development policy, with the goal to reduce poverty, ensure sustainable development, and promote democracy, human rights, and the rule of law across the world.

The mission of the Ministry of Foreign Affairs of Estonia, , is to make sure that Estonia's security and well-being is ensured and to protect Estonia´s interests in the world by planning and implementing foreign policy and coordinating foreign relations. In terms of Cyber Capacity building, Estonia has supported the development of cyber security systems in developing and partner countries for over ten years and will continue to do so in the future.

e-Governance Academy (eGA) is a centre of excellence for increasing the prosperity and openness of societies through digital transformation. Over the last 20 years, eGA has collaborated with more than 280 organisations and 141 countries on digital innovations and assisted government organisations of Albania, Moldova, Montenegro, Uganda, Turkiye, and Ukraine in improving national cybersecurity and enhancing cyber frameworks and skills. Since 2016, eGA develops and manages the National Cyber Security Index (NCSI), ncsi.ega.ee, - a tool for measuring countries preparedness to mitigate cyber threats and manage cyber incidents and build national cybersecurity capacity.

Estonian Centre for International Development (ESTDEV), is a government-founded and funded organisation created to manage and implement Estonia's development cooperation programs and Estonia's participation in global development initiatives. By sharing Estonia's successful reform experience in digital transformation, ESTDEV promotes safe, transparent and humancentric e-services in all areas.

www.tallinncyberdiplomacy.ee