Tallinn Cyber Diplomacy Summer School 2026

# Tallinn Cyber Diplomacy Summer School

Concept Note

The evolution of the digital environment and associated risks that transcend national borders bring to the fore the importance of international cooperation and the role of cyber diplomacy. Cybersecurity and digitalisation are increasingly central to regional and global efforts to advance the digital economy, trusted connectivity, and progress towards sustainable development goals. Therefore, a better understanding of the challenges posed by state-sponsored cyber operations, cybercrime, and the strategic impacts of emerging technologies such as AI is a key aspect of modern diplomacy. The need for cohesive global collaboration and governance has never been more critical.

The seventh edition of The Tallinn Cyber Diplomacy Summer School 2026 will explore these essential topics, 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 safe, secure, resilient, and open cyberspace.

## Participants

This five-day event is designed for diplomats, government officials and experts who are involved or demonstrate clear interest in cyber policy, cyber diplomacy, or international cyber cooperation. The course offers government officials and policymakers at all levels a unique opportunity to deepen their understanding of complex, multifaceted cyber issues and become members of a vibrant Tallinn Cyber Diplomacy community.

## 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 Mövenpick Hotel Tallinn, a modern four-star business and conference hotel, ideally located in the heart of Tallinn, with easy access to the picturesque historic 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

estdev From the people of Estonia

## Topics and Agenda

Participants will engage in in-depth discussions at the intersection of foreign policy, digital governance and technology, examining the evolving cyber landscape, the implications of emerging technologies, strategies for critical infrastructure protection, frameworks for international stability, challenges such as cybercrime, and the importance of capacity building, while also exploring the cyber policies and practices of regional and international organizations.

### Day 1

The first day of the course will establish the context 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 are the key challenges of contemporary digital transformation, especially regarding connectivity and infrastructure projects? What are the main risks and threats to digitalization, especially regarding aspects such as satellite connectivity and security of ICT supply chains in the context of geopolitical competition among major powers? What are the 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

The second day focuses on the international cybersecurity landscape, examining the frameworks and mechanisms that govern state behavior in cyberspace. Participants will gain a comprehensive understanding of the cyber diplomacy environment and the key concepts necessary to engage effectively in global discussions. Participants will explore the core elements of the UN framework for responsible state behavior in cyberspace, assessing future challenges and opportunities to strengthen its development, implementation, and ongoing relevance, and provide a forward-looking analysis in relation to the launch of the UN Global Mechanism. It will explore how to preserve the progress achieved by the international community and address the outstanding controversies. Sessions will also cover emerging multilateral mechanisms beyond the mandate of the UN Global Mechanism. A panel discussion with cyber ambassadors will provide practical insights into how diplomats navigate these frameworks, enhance their impact on international platforms, and leverage evolving international cooperation to strengthen cyber stability.

### Day 3

The third day will be dedicated to implementing cybersecurity frameworks, their implications for local contexts, and ways to better integrate these advancements at national and regional levels. Participants will examine how states operationalise responsibility in cyberspace, including attribution processes, accountability for malicious actors, and the role of national cyber resilience in preventing and mitigating cyber crises. The sessions highlight how existing diplomatic tools and stability frameworks can be translated into actionable national strategies. Additionally, participants will gain insight into collective cyber defense and diplomatic frameworks, including those of the EU

and NATO, understanding how these mechanisms can be used to strengthen both national and regional cybersecurity posture.

## Day 4

The fourth day provides hands-on insight into leveraging cybersecurity capacity-building initiatives to enhance national and regional resilience. Participants will explore the interconnections between capacity building, the implementation of international stability frameworks, and cyber diplomacy. Practical sessions will demonstrate how diplomats and cyber experts can align capacity-building efforts with national priorities, optimize their impact, and contribute to more robust, coordinated regional and international cyber resilience. The sessions examine 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.

## 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. 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. The workshop aims to bridge theoretical knowledge with practical skills, preparing participants to make informed, strategic decisions. 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 practical dialogue with relevant cybersecurity and/or government entities. These discussions provide practical insights into the operations and strategies employed in cybersecurity.

The program also includes a hands-on cybersecurity table-top 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

The Tallinn Cyber Diplomacy Summer School is an initiative funded by the European Union under the Global Gateway. The Global Gateway stands for sustainable and trusted connections that work for people and the planet. It helps to tackle the most pressing global challenges, from fighting climate change, to improving health systems, and boosting competitiveness and security of global supply chains.

The Tallinn Cyber Diplomacy Summer School is implemented through a partnership among several organizations.

**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 are 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 cybersecurity 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