Tallinn Cyber Diplomacy Winter School 2025

Tallinn Cyber Diplomacy Winter School 2025!

The Tallinn Cyber Diplomacy Winter School is designed to strengthen the Tallinn Cyber Diplomacy Summer School Alumni network. The 3-day gathering, taking place on 10-12 March 2025 in **Santo Domingo, the Dominican Republic**, will allow the Alumni to deepen their professional connections, exchange regional insights, and address pressing cyber diplomacy challenges through focused discussions, expert-led sessions, and collaborative activities.

Each Winter School will focus on different region-specific priorities, with input from the Alumni shaping the agenda to ensure relevance and practical impact. The 2025 edition focuses on the Latin American region. By fostering dialogue, sharing expertise, and promoting EU values, the Winter School aims to advance a free, open, secure, and resilient cyberspace globally.

The Tallinn Cyber Diplomacy Winter School 2025 is co-organised by the European Commission's Directorate-General for International Partnerships (DG INTPA), the Estonian Ministry of Foreign Affairs, the e-Governance Academy (eGA), and EU CyberNet.

It is hosted at the Latin America and Caribbean Cyber Competence Centre (LAC4), implemented by EU CyberNet and funded by the European Union. Established in 2022, LAC4 features a dedicated physical training facility in Santo Domingo, serving as a vital hub for cyber capacity-building in the region.

Global Gateway

Republic of Estonia
Ministry of Foreign Affairs

eGA e-governance academy

EU CyberNet

* The organisers reserved the right to adjust the program elements and venues outlined in the draft agenda, ensuring that these adjustments do not affect the program's focus or goals.

Topics

Day 1 (10 March) — International stability framework — from global norms to national implementation

Theme: This day will build upon the February 2025 session of the OEWG, offering a comprehensive summary of achievements from the past four years and examining the ongoing progress of the OEWG process. Discussions will highlight recent developments in the international cyber stability framework, their implications for local contexts, and ways better to integrate these advancements at national and regional levels. The sessions will also encourage practical dialogue on leveraging the OEWG process to address local needs and challenges.

Moderator of the day: **Claudio Peguero**, Ambassador, Advisor on Cyber-matters, Ministry of Foreign Affairs, the Dominican Republic

Day 2 (11 March) — Cyberthreats and how Cybersecurity Governance models can help mitigate them

Theme: This day will focus on regional perspectives, highlighting the best cybersecurity governance and collaboration practices. The agenda will explore the evolving threat landscape from various angles, including national and private sector perspectives. It will offer case studies and examine how emerging technologies like 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: **Merle Maigre,** Head of Cybersecurity Competence Center, e-Governance Academy

Day 3 (12 March) — Practical workshop: We depend on each other: now what?

Theme: Addressing regional cross-border (inter)dependencies in cooperation and collaboration

The final day is dedicated to applying the knowledge and skills through a practical workshop/scenario-based discussion, so participants are equipped to actively engage in the discussions within their respective national contexts. Participants will explore how nations can strategically address cross-border digital dependencies in an increasingly interconnected region, focusing on identifying critical interdependencies, understanding their impact on national and regional resilience, and fostering international cooperation to manage these challenges.

Through practical, interactive discussions, participants will better understand national/regional real-world cross-border dependencies and understand their implications and develop actionable strategies for addressing them. By the end of the session, participants will be better equipped to contribute to national cybersecurity strategies and regional discussions, aligning governance and cooperation models with real-world challenges and opportunities.

Organisers:

The Tallinn Cyber Diplomacy Winter School 2025 is co-organised by the European Commission's Directorate-General for International Partnerships (DG INTPA), the Estonian Ministry of Foreign Affairs, the e-Governance Academy (eGA), and EU CyberNet.

DG INTPA — European Commission's Directorate-General for International Partnerships

DG INTPA is responsible for designing and implementing the European Union's international partnerships and development cooperation policies, promoting global stability, prosperity, and resilience. It plays a key role in supporting digital transformation and cybersecurity capacity-building efforts worldwide.

The Ministry of Foreign Affairs of Estonia

The Ministry of Foreign Affairs of Estonia ensures Estonia's security and well-being by advancing its interests globally through strategic foreign policy and international cooperation. Estonia has been actively supporting cyber capacity building in developing and partner countries for over a decade and remains committed to enhancing global cybersecurity resilience.

The e-Governance Academy (eGA)

eGA is a centre of excellence dedicated to increasing societal prosperity and transparency through digital transformation. Over the past 20 years, eGA has collaborated with over 280 organisations across 141 countries, assisting governments in improving national cybersecurity and enhancing cyber frameworks and skills. Since 2016, eGA has been developing and managing the National Cyber Security Index (NCSI) — a global tool measuring countries' preparedness to mitigate cyber threats and manage cyber incidents (ncsi.ega.ee).

EU CyberNet

The European Union External Cyber Capacity Building Network (EU CyberNet) was launched in 2019 to strengthen the EU's global cybersecurity efforts. Its mission is to enhance the coordination and effectiveness of EU-funded cyber capacity-building initiatives while fostering a network of cyber experts to support third countries. Led by the Estonian Information System Authority in partnership with Finland, Germany, and Luxembourg, EU CyberNet ensures that the EU remains at the forefront of cyber diplomacy and global cybersecurity development.