Tallinn
Summer School
of Cyber Diplomacy
2024

**Upholding a free, open, safe and secure cyberspace**

11-15 November

DRAFT AGENDA*

# Tallinn Summer School of Cyber Diplomacy 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.

Global Gateway

Republic of Estonia
Ministry of Foreign Affairs

eGA
e-governance academy

estdev
From the people of Estonia

* 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 and Agenda

## Day 0 (10 November) — Icebreaker at POCO in Rotermann City
## 19:00 — 22:00

## 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.

| Morning session \| 9:00-14:00 \| Hotel Nordic Forum | |
|---|---|
| 9:00-9:30 | Registration and gathering |
| 9:30-10:15 | Opening remarks |
| 10:15-11:00 | The case for digitalisation as an enabler. Why does digitalisation matter, why does cybersecurity matter to digitalisation?<br>15 min introduction + conversation between panellists moderated by the moderator of the day |
| 11:00-11:30 | Coffee break/networking |
| 11:30-12:30 | Global cyber threats and trends, role of AI in the threat landscape. Insights from global defenders in industry.<br>15/20 min introduction + conversation between panellists moderated by the moderator of the day +Q&A |
| 12:30-14:00 | Lunch |

* 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.

<table>
<tr><th colspan="2">Afternoon session | 14:00-16:45 | Hotel Nordic Forum</th></tr>
<tr><td>14:00-14:45</td><td>National cyber threat landscape. Vulnerabilities and threats, actors and risks.</td></tr>
<tr><td>14:45-15:30</td><td>Incident response for policymakers</td></tr>
<tr><td>15:30-16:00</td><td>Coffee break/networking</td></tr>
<tr><td>16:00-16:45</td><td>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)</td></tr>
<tr><th colspan="2">Evening programme | 17:30-22:30 |</th></tr>
<tr><td>17:30-22:30</td><td>Fire site 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 future-proofing.</td></tr>
<tr><td></td><td>Dinner</td></tr>
<tr><td>22:30</td><td>Transfer back to the Hotel</td></tr>
</table>

## 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.

<table>
<tr><th colspan="2">Morning session | 9:00-14:00 | Hotel Nordic Forum</th></tr>
<tr><td>9:00-9:30</td><td>Keynote: The international cyber stability framework. The role for Cyber Diplomacy.</td></tr>
</table>

* 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.

| | |
|---|---|
| 9:30-10:30 | Norms of responsible state behaviour and cyber security confidence building measures.<br>Short opening statements (5-7 min) + panel discussion + Q&A (10 min) |
| 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.<br>Short opening statements (5-7 min) + panel discussion + Q&A (10 min) |
| 12:00-13:30 | Lunch |
| Afternoon session \| 14:00-17:00 \| | |
| 13:30-14:00<br>14:00-14:45 | Implementing the cyber stability framework: the UN (in) action<br>The geopolitics of technology. The rise of digital diplomacy. |
| 14:45-15:30 | Protecting and promoting human rights online and offline. |
| 16:00-18:00 | Guided City tours (pre-registration) |
| Evening programme \| 18:00-22:30 \| Lennusadam, Vesilennuki 6, Tallinn | |
| 18:00 | Gathering at hotel lobby, transfer<br>Fire site chat and dinner |
| 21:30 | 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

* 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.

stability frameworks. The session will also introduce collective diplomatic and cyber defence frameworks of the EU and NATO.

| | |
|---|---|
| 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? |
| 9:30-10.30 | Mechanisms of state accountability. Case studies from the European Union and NATO. |
| 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.<br>Panel discussion. |
| 12:30-13:30 | Lunch |
| Afternoon session \| 13:45-18:00 \| | |
| 13:30-14:15 | How to write a national position on the applicability of International Law in cyberspace. |
| 14:15-14:45 | Building national resilience: what is national digital and cyber resilience ecosystem. Objectives, principles, and architecture of national cybersecurity from a national perspective. |
| 15:00-18:00 | Transfer to the field visit in two groups<br>Group A - Field visit to (Defence League Cyber Defence Unit, MOD, Defence League, Defence Forces)<br>Group B — Field visit to CCDCOE |
| Evening programme \| Teras Beach \| Tallinn Indoor Beach | |
| 19:00 | Gathering in hotel lobby, transfer to Tallinn Indoor Beach (Address Lõuka 6) |
| 19:30 | Dinner discussion: Cyber ambassadors' perspective. |
| 23:00 | Transfer back to the Hotel |

* 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.

## 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.

<table>
<tr><th colspan="2">Morning session | 9:00-12:15 | Hotel Nordic Forum</th></tr>
<tr><td>9:00-9:15</td><td>Contextualising capacity building - Aspects, approaches and strategies. Understanding the links between cyber resilience, cyber capacity building and cyber stability frameworks.</td></tr>
<tr><td>9:15-10:15</td><td>Panel discussion: Cybersecurity capacity building in practice: Regional priorities, challenges, and lessons learned: Donor/Implementer perspective.</td></tr>
<tr><td>10:15-10:45</td><td>Coffee break/networking</td></tr>
<tr><td>10:45-11:45</td><td>Cybersecurity capacity building as a diplomatic priority in practice: Challenges, lessons learned and global and regional priorities: Beneficiary perspective.</td></tr>
<tr><td>11:45-12:15</td><td>National Cyber Security Index — Understanding and Leveraging the NCSI for maximum benefit.</td></tr>
<tr><td>12:30-14:30</td><td>Gathering at hotel lobby walk to restaurant<br>Lunch Restaurant OLDE HANSA (Address: Vana turg 1, Tallinn Old town)</td></tr>
<tr><td colspan="2">Afternoon session | 14:40 — 17:00 | Vabamu Museum of Occupations and Freedom</td></tr>
<tr><td>14:30-15:30</td><td>Case study: Tallinn Mechanism</td></tr>
<tr><td>15:30-16:00</td><td>Coffee break</td></tr>
<tr><td>16:00-17:00</td><td>Case study: Story of Estonia´s reform through digitalisation and cybersecurity.</td></tr>
</table>

Global Gateway

Republic of Estonia
Ministry of Foreign Affairs

eGA
e-governance academy

estdev
From the people of Estonia

* 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.

# 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.

<table>
<tr><th colspan="2">Morning session | 9:00-12:30 | Hotel Nordic Forum</th></tr>
<tr><td>09:00-12:30</td><td>Practical workshop<br>Table-top exercise<br>Including Coffee break/networking</td></tr>
<tr><td>12:30-13:30</td><td>Lunch</td></tr>
<tr><td>13:30</td><td>Gathering at the Hotel lobby. Walk to the MFA.</td></tr>
<tr><th colspan="2">Afternoon session | 14:00-16:00 | Ministry of Foreign Affairs</th></tr>
<tr><td>14:00-15:30</td><td>Keynote speech: Minister of Foreign Affairs<br>Conclusions of the Summer School<br>Handover of diplomas. Minister of Foreign Affairs of the Republic of Estonia</td></tr>
<tr><td>15:30 — 17:00</td><td>Networking reception</td></tr>
</table>

Global Gateway

Republic of Estonia
Ministry of Foreign Affairs

eGA
e-governance academy

estdev
From the people of Estonia

* 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.