DRAFT AGENDA* 11.05.2026

Tallinn Cyber Diplomacy Summer School

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 need for cohesive global collaboration and governance has never been more critical. The Tallinn Cyber Diplomacy Summer School was established to support government officials in deepening their knowledge of key concepts and mastering the tools of modern diplomacy to become effective agents of change in their countries.

The seventh edition of The Tallinn Cyber Diplomacy Summer School will explore the most essential themes, providing a platform for diplomats, experts and policymakers to enhance their understanding, skills and role in navigating the complex cyber domain, and build a cross-regional community of cyber diplomacy experts. It provides a dynamic, high-level program for young cyber professionals, diplomats, and public officials worldwide. Over five intensive days, participants will engage in expert-led sessions, hands-on exercises, and networking with peers and global thought leaders. Building on the success of previous years, this event continues to foster a safe, secure, resilient, and open cyberspace. The Tallinn Cyber Diplomacy Summer School is part of the **EU-funded Tallinn Cyber Diplomacy Programme**, which promotes global cyber resilience capacity-building and aligns with the EU's core values of democracy, human rights, and the rule of law. It supports the EU's strategic commitment to inclusive multilateralism and a secure, open digital future.

The Summer School is co-organised by the **e-Governance Academy (Estonia), European Commission (DG INTPA), the Ministry of Foreign Affairs of Estonia, and supported also by ESTDEV.**

The organisers reserved the right to adjust the program 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 (14 June) — Icebreaker at 19:00 — 21:30

Day 1 (15 June) — Digital, New Tech and Cybersecurity Nexus. Shifting Paradigms and Policy Challenges

Theme: The first day 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.

Moderator of the day: ***Elina Noor,*** Non-resident Scholar, Asia Program, Carnegie Endowment for International Peace

Morning session | 9:00 - 14:00 |	
8:30 - 9:00	Registration and gathering
9:00 - 9:45	**Opening remarks**

*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.

09:45 - 10:30	**Securing the digital transformation: safeguarding growth and resilience** The rapid evolution of digital technologies — from artificial intelligence and quantum computing to cloud ecosystems — is reshaping economies, governance, and global power dynamics. This session explores how emerging technologies both enable progress and generate new cyber risks, requiring adaptive and forward-looking policy responses. Participants will examine how digital transformation influences national competitiveness, economic security, and international cooperation in cyberspace.
10:30 - 11:30	**Derisking global connectivity: policy priorities for secure critical infrastructure** The resilience of the global Internet depends on complex physical and digital systems — from subsea cables and satellite networks to 5G hardware and telecommunications software. As geopolitical tensions and supply chain dependencies intensify, ensuring the security of these infrastructures has become a strategic priority for infrastructure investments and international partnerships. This session explores policy approaches to derisking critical connectivity layers, enhancing trust and resilience through technological diversification, transparency, and international cooperation.
11:30 - 12:00	Coffee break & networking
12:00 - 13:00	**Navigating the cyber threat landscape: trends, actors, and policy responses** The cyber threat environment is becoming increasingly complex, with state and non-state actors exploiting vulnerabilities across critical sectors. Ransomware attacks, supply chain compromises, and disruptive intrusions now challenge both national security and public trust. This session examines current threat trends, the motivations and methods of key actors, and the policy mechanisms that can enhance resilience and deterrence in this evolving landscape.
13:00 - 14:00	Lunch
Afternoon session | 14:00 - 17:00 |	
14:00 - 14:45	**AI and cyber power: the next frontier of digital strategy**Artificial intelligence is rapidly transforming cybersecurity, diplomacy, and the

*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.

	balance of power in the digital age. As an enabler and amplifier, AI enhances defensive capabilities, streamlines threat detection, and supports decision-making — yet it also introduces new risks. This session examines the state of play in AI development, its applications across public and critical sectors. Participants will explore how governments can harness AI's potential responsibly while addressing security, ethical, and governance challenges.
14:45 - 15:30	**Governing emerging technologies: aligning global policy approaches** Emerging technologies like artificial intelligence are reshaping global governance and testing existing international frameworks. As AI becomes integral to economic growth, security, and public administration, the need for coherent and principled policy approaches is more pressing than ever. This session explores how cyber diplomats and international policy actors can shape global responses to AI governance through collaboration, alignment, and shared norms.
15:30 - 15:45	Coffee break & networking
15:45 - 16:30	**Strengthening sustainable and trusted investments in digital economy** As the digital economy expands, trust and sustainability have become central to secure and inclusive growth. Governments and the private sector alike face pressure to ensure that digital infrastructure, technologies, and supply chains are built on transparency, accountability, and resilience. This session explores how trusted providers, responsible innovation, and diversified partnerships can drive sustainable investment in the digital space through increased cybersecurity by design. Participants will discuss policy tools that promote secure digital value chains while encouraging innovation and competitiveness in emerging markets.
16:30 - 17:00	**National Cyber Security Index: why measuring matters** This session offers a strategic view of the National Cyber Security Index (NCSI) as a tool to assess, understand, and strengthen national cyber capacities and ensure sustainable, secure and trustworthy digital transformation. Participants will explore how to leverage the NCSI to support policymaking, track progress, and align with international cyber stability and capacity-building efforts.
Evening programme | 18:00 - 22:30 |	

Global Gateway · Republic of Estonia Ministry of Foreign Affairs · eGA · estdev

*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.

18:30 - 19:30	**Fireside Chat:** Who controls the future? A discussion on balancing rapid technological advancement, human agency, and global security in the age of AI?
19:30 - 21:45	**Dinner and networking**

Day 2 (16 June) — Cyber diplomacy and international cybersecurity frameworks

Theme: 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.

Moderator of the day: ***Taimar Peterkop,*** Senior Expert on Cybersecurity at the e-Governance Academy

Morning session | 9:00 - 14:00 |	
9:00 - 9:30	**Keynote: Cyber stability in a fragmented world – the role of cyber diplomacy** As geopolitical tensions extend into the digital domain, achieving and maintaining cyber stability has become increasingly complex. Competing models of governance, divergent norms, and rapid technological change challenge the coherence of the international cyber stability framework. This keynote examines where global efforts stand today and how cyber diplomacy can bridge divides, foster dialogue, and build consensus toward a secure, open, and cooperative cyberspace.

*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 - 10:15	**Shaping global responses to cybercrime and intrusion tools** The rise of cybercrime and the proliferation of commercial cyber intrusion tools are reshaping global security and governance. Addressing these challenges requires coordinated international action grounded in human rights, transparency, and accountability. This session spotlights key initiatives — including the Counter Ransomware Initiative (CRI), the UN Ad Hoc Committee on Cybercrime, and the Pall Mall Process — exploring how each contributes to building responsible state behavior and curbing the misuse of cyber capabilities.
10:15 - 10:45	Coffee break & networking
10:45 - 11:30	**Safeguarding digital resilience in an era of control** Across the globe, authoritarian regimes cite national security concerns to justify restrictive digital measures — from Internet shutdowns and content filtering to practices such as whitelisting and platform blocking. While governments seek to manage risks and maintain stability, these actions often disrupt essential services, constrain economic activity, and erode public trust. This session explores how states can uphold security and public order without undermining connectivity, openness, or human rights online and what common action is needed to push back against authoritarian opractices. Participants will discuss policy approaches that promote resilient, rights-respecting, and interoperable digital ecosystems. **Learning objective:** Evaluate how policy choices surrounding Internet control measures affect digital resilience and identify strategies to safeguard secure, open, and trusted online environments.
11:30 - 12:30	**Global Mechanism: a new chapter in multilateral cyber diplomacy** As cyberspace becomes a central arena of geopolitics, efforts to establish shared frameworks for stability and security are entering a new phase. The recently launched Global Mechanism marks a milestone in international cooperation on responsible state behavior, confidence-building, and capacity-sharing in the cyber domain. This session examines the objectives and diplomatic significance of the Mechanism, exploring how it can strengthen global coordination, reduce the risk of conflict, and reinforce trust among nations.

*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.

	Learning objective: Understand the role of the Global Mechanism in advancing multilateral cyber diplomacy and shaping a more stable, predictable, and cooperative international environment.
12:30	Family Photo
12:45 - 13:45	Lunch
Afternoon session | 13:45 - 15:45 |	
13:45 - 14:30	**Norms of responsible state behaviour in cyberspace** At the heart of the UN framework of responsible state behaviour lies a set of voluntary, non-binding norms guiding how states should act responsibly in cyberspace. Developed through UN processes such as the GGE and OEWG, these norms seek to ensure that cyberspace remains open, secure, and stable. This session offers a concise overview of the purpose and practical significance of these norms, providing participants with the conceptual grounding to understand their role within the broader UN framework of responsible state behaviour.
14:30 — 15:00	**Confidence-building measures: building trust and transparency in cyberspace** Confidence-Building Measures (CBMs) are practical tools for reducing misunderstanding and preventing escalation in cyberspace. They foster communication, transparency, and cooperation among states through information sharing, incident reporting, and bilateral or regional dialogue. This session explores the evolution of cyber CBMs within the UN and regional organisations, illustrating how they enhance predictability and trust in an increasingly contested digital environment.
15:00 - 15:30	Coffee break & networking

*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.

15:30 - 16:15	**International law in cyberspace: principles, application, and practice** International law provides the legal foundation for responsible state conduct in cyberspace. While its applicability is widely recognised, differing interpretations continue to shape international discussions on sovereignty, due diligence, and self-defence in the digital domain. This session introduces the main legal principles relevant to cyberspace and explores how states articulate and implement them through national positions, regional initiatives, and multilateral dialogue.
16:15 - 17:00	**Developing national positions on the applicability of international law in cyberspace** Formulating a national position on how international law applies to state behaviour in cyberspace is a crucial step toward transparency, predictability, and international dialogue. Such statements clarify states' legal interpretations and contribute to shaping common understanding within multilateral fora. This session provides a practical framework for policymakers and diplomats on how to develop, structure, and communicate these positions — addressing key legal concepts such as sovereignty, due diligence, and the use of force. Participants will explore existing examples and discuss how consistent, well-articulated positions can strengthen national influence and support global stability.
Evening programme | 18:15 - 22:30 |	
19:00 - 20:00	**Fireside chat session: Artificial intelligence and the internal processes of creativity**
20:00 - 22:00	**Dinner and networking**

*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 3 (17 June) — Cyber diplomacy in action: approaches, instruments and tools

Theme: 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.

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

Morning session | 09:00 - 13:00 |	
09:00 - 09:30	**Cyber capabilities in modern conflicts: evolving threats and policy responses** Cyber operations have become an integral feature of modern conflict, shaping both the conduct and outcomes of crises across physical and digital domains. From strategic disruption to information manipulation, offensive and defensive cyber capabilities are now key instruments of state power and deterrence. This session examines the evolving role of cyber capabilities in contemporary conflicts, exploring their impact on military strategy, escalation dynamics, and international security.
09:30 - 10:30	**Diplomatic responses to malicious cyber activity: balancing legal, technical, and political tools** Responding effectively to malicious cyber activity requires a careful balance between legal principles, technical evidence, and political judgment. Governments face complex choices when attributing responsibility, imposing consequences, or engaging through diplomatic channels. This session

*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.

	explores the spectrum of available response options — from public attribution and sanctions to cooperative incident management and dialogue — and considers how states weigh proportionality, legitimacy, and strategic effect.
10:30 - 11:00	Coffee break & networking
11:00 - 12:00	**Strengthening accountability in an era of hybrid cyber threats** As hybrid operations increasingly blend cyber, information, and geopolitical tactics, ensuring accountability in cyberspace has become both more urgent and more complex. The use of proxies and commercial actors to mask responsibility challenges existing policy and legal frameworks, demanding more agile and coordinated responses. This session looks ahead to emerging models of accountability — from collective attribution and joint response mechanisms to strengthened transparency and due-diligence standards. Participants will explore how future policy architectures can deter cyber and hybrid threats and reinforce responsible state behaviour.
12:00 - 13:00	Lunch
Afternoon session | 13:00 - 17:00 |	
13:00 - 14:00	**Cyber capacity-building priorities for the UN Global Mechanism** For the UN Global Mechanism to succeed, it must focus on the capacity-building priorities that address the most pressing and diverse needs of states. This session explores how the Mechanism can set clear goals to support national and regional resilience — from strengthening institutional frameworks and crisis response capabilities to developing skilled workforces and promoting secure connectivity. Participants will identify key areas where coordinated international support can deliver the greatest impact, ensuring that capacity-building efforts are inclusive, sustainable, and responsive to global demand. Learning objective: Define priority goals for the UN Global Mechanism to ensure that cyber capacity-building initiatives effectively meet the evolving needs of states and regions.
14:00 - 14:45	**Strengthening national resilience: putting the UN framework into practice**.

*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.

	Translating the UN framework of responsible state behaviour into national action is essential for building a secure and resilient digital environment. Implementing its principles — from norms and international law to confidence- and capacity-building measures — requires coordinated engagement across government, industry, and civil society. This session explores practical approaches for operationalising the framework at the national level, including policy alignment, institutional coordination, and cross-sector partnerships.
14:45 — 15:15	Coffee break & networking
15:15 - 17:00	**Group discussions: National priorities and the UN Global Mechanism** Building on the concepts explored throughout the programme, this interactive session invites participants to reflect on how the emerging UN Global Mechanism aligns with their national priorities, challenges, and strategic objectives. In small groups, participants will discuss opportunities for engagement, capacity-building, and cooperative action under the Mechanism's framework. The exercise will encourage exchange of perspectives across regions and levels of development, fostering a practical understanding of how global initiatives can support national implementation and resilience.
Evening programme | 17:30 - 22:00 |	
18:00	**Trustbuilders in a fragmented cyberspace: reflections from the frontlines of cyber diplomacy** This evening panel brings together cyber ambassadors and senior diplomats for a candid conversation about the human dimension of cyber diplomacy — how relationships, credibility, and persistence shape negotiations on some of today's most complex digital challenges. Through personal insights and diplomatic anecdotes, speakers will reflect on what it takes to build confidence across divides, sustain dialogue amid tension, and keep communication channels open when trust is in short supply.
19:00 - 22:00	Dinner and networking

*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 (18 June) — Building cyber resilience through diplomacy: cyber norms implementation providing a vision for the cyber capacity building

Theme: 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.

Moderator of the day: ***Merle Maigre****, Director of Cybersecurity Competence Centre, e-Governance Academy*

Morning session | 09:15 - 12:35 |	
09:00 - 09:45	**Cyber capacity building: state of play and emerging directions** Cyber capacity building has become a cornerstone of international efforts to enhance resilience, bridge capability gaps, and promote responsible state behaviour. Yet as the cyber threat landscape and technological dependencies evolve, capacity-building approaches must adapt to new realities. This session takes stock of current global initiatives, examining lessons learned and emerging trends — from integrating capacity-building into development cooperation to enhancing sustainability and local ownership. Participants will explore new strategies for aligning national, regional, and multilateral efforts to meet future resilience and security needs.
09:45 — 10:45	**Cyber capacity building: lessons from strengthening global cyber resilience** Building and sustaining cyber capacity is essential for enabling states to protect their digital infrastructures, respond to threats, and participate effectively in international cyber stability efforts. Beyond inclusion, capacity-building focuses on developing baseline institutional, technical, and

*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.

	human capabilities that allow governments to detect, prevent, and mitigate cyber incidents. This session explores guiding principles for effective and sustainable capacity-building — emphasising national ownership, trust-based partnerships, and the importance of aligning assistance with broader security and development objectives.
10:45 — 11:15	Coffee break & networking
11:15 - 12:00	**Bridging the cyber divide: connectivity, security, and resilience** Closing the digital divide depends not only on expanding access but also on ensuring that connectivity is secure, reliable, and sustainable. This session examines how global infrastructure initiatives and capacity-building efforts can strengthen cyber resilience by integrating cybersecurity and critical infrastructure protection from the ground up. Experts will discuss challenges related to cross-border dependencies, supply chain security, and trusted technology providers, exploring whether current strategies are sufficient to safeguard connectivity in an increasingly interconnected world.
12:00 - 13:00	**Financing cyber resilience: investment strategies and the role of the private sector** Securing a resilient digital ecosystem requires sustained investment in cybersecurity, infrastructure, and innovation. Private capital and international financial instruments play a critical role in scaling these efforts, especially in emerging markets where capacity gaps remain significant. This session examines how targeted investment, blended finance, and risk-sharing models can advance cybersecurity goals while promoting economic development and trust. Participants will discuss how cooperation between investors, governments, and development institutions can unlock financing for secure and sustainable digital growth.
13:00 - 14:00	Lunch
Afternoon session | 14:00 - 17:00 |	
14:30 - 15:00	**Tour in Vabamu**

*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.

15:00 - 16:30	**Case Study:** Cyber Assistance to Ukraine - the role of public-private partnerships in building national cyber resilience: Tallinn Mechanism and IT-Coalition.
19:30 - 22:00	Free evening Optional: Buffee dinner at the hotel (pre-registration needed)

Day 5 (19 June) — Practical workshop, exercise and wrap-up

Theme: The final day is dedicated to applying the knowledge and skills learned through a practical 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.

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

Morning session | 09:00 - 12:30 |	
09:00 - 12:30	**Practical workshop / Table-top exercise** Including Coffee break & networking
12:30 - 13:30	Lunch
Afternoon session | 14:00 - 17:00 |	
14:15	**Keynote speech and Conclusions**
15:00	**Handover of diplomas**
15:30 - 17:00	Networking reception in the Ministry of Foreign Affairs 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.