Tallinn
Cyber Capacity-Building
Fellowship Programme
2026

Call for Applications
Cyber Capacity-Building Fellowship 2026

Dates: 7—18 September 2026

1 week online, 7—10 September

1 week in-person in Tallinn and Tartu, Estonia, 14—18 September

About the Fellowship

The rapid expansion of digital technologies and the growing influence of artificial intelligence (AI) are reshaping the global cybersecurity landscape, creating new opportunities as well as increasingly complex risks for states, institutions, and societies. As AI capabilities become more integrated into governance, critical infrastructure, and cyber operations, cybersecurity professionals and cyber diplomats require a stronger understanding of both the security implications and policy dimensions of emerging technologies. At the same time, evolving cyber threats, including state-sponsored cyber operations, cybercrime, and the misuse of emerging technologies continue to highlight the importance of international cooperation, cyber resilience, and effective global cyber governance.

Organised annually, the **Cyber Capacity-Building Fellowship Programme** is designed to equip junior and mid-level cybersecurity professionals and cyber diplomats from the EU global partner countries with the skills, insights, and networks needed to tackle today's most pressing cybersecurity challenges. While maintaining its core focus on strengthening cybersecurity expertise, the Fellowship Programme will also explore the policies, opportunities and risks related to AI. Through practical exchanges and multi-stakeholder engagement, the programme seeks to support the development of informed, adaptable, and globally connected cyber professionals capable of contributing to free, open, safe, and secure cyberspace.

The second edition of the Fellowship Programme will take place from **7—18 September 2026**, featuring one week of light interactive online learning (7—10 September), followed by one week of in-person engagement in **Tallinn and Tartu, Estonia** (14—18 September) — internationally recognised hubs for digital innovation and cyber governance.

Participants will benefit from direct interaction with leading practitioners across government, international organisations, academia, the private sector, and civil society, fostering practical knowledge exchange and long-term professional networks across the global cybersecurity community.

Global Gateway

eGA e-governance academy

Tallinn
Cyber Capacity-Building
Fellowship Programme
2026

Key Themes and Learning Areas

Fellows will engage with a wide range of topics, including:

- **Cybersecurity Policy and Governance:** National strategies, national and international regulatory frameworks, EU policies and best practices
- **Cyber Diplomacy and International Cooperation:** Cyber norms, international law, state accountability, confidence-building measures and capacity-building initiatives
- **Artificial Intelligence and Cybersecurity:** The current state of AI development, its applications across public and critical sectors, and policy frameworks to promote trusted, inclusive and sustainable use of AI.
- **Legal and Ethical Aspects of Cybersecurity:** Human rights online, data protection, digital rights
- **Cyber Threat Landscape:** Cyber threat landscape, risk assessment and mitigation, incident response, critical infrastructure security
- **Multi-Stakeholder Collaboration:** Roles of civil society, academia, private sector, and public-private partnerships

Through expert-led lectures and discussions, hands-on workshops, and real-world case studies, the Fellowship will prepare participants to apply knowledge effectively at the national and international levels.

Expected Outcomes

By the end of the Fellowship, participants will:

- Develop enhanced skills in cybersecurity policy and cyber diplomacy;
- Gain exposure to EU cyber governance models and global best practices;
- Improve awareness of current AI developments and their implications for cybersecurity, digital governance, and critical infrastructure resilience.
- Join a growing Fellowship alumni network and access fellow cybersecurity experts worldwide;
- Contribute to global dialogue on cybersecurity and resilience;
- Complete an individual, National Cyber Security Index (NCSI) based review of national cybersecurity capacities and contribute to a collaborative presentation on cybersecurity capacity-building challenges and good practices.

Programme Structure and Methodology

Tallinn Cyber Capacity-Building Fellowship Programme 2026

The Fellowship follows a blended learning methodology that combines policy discussions, expert insights, technical training, and peer learning. The programme includes a two-part practical assignment designed to translate the acquired new knowledge into practical outcomes, which are relevant to the participants' professional work. During the online component, fellows will complete an individual task based on the NCSI methodology, reviewing and validating country-level data for their country. During the in-person week, fellows will work in groups to develop and deliver a presentation on key cybersecurity topics. This blended approach ensures both individual reflection and collaborative application of knowledge.

The **first week of the programme** (7—10 September, **online**) will provide participants with a theoretical foundation through a series of interactive lectures and an introduction to the Fellowship's practical assignment, guidance on the use of the NCSI methodology, and the requirements for both individual and group tasks.

The online component will consist of four focused sessions, each featuring one or two 30-minute expert presentations, followed by Q&A segments, with a total duration of no more than 90 minutes per session. These sessions are designed to prepare the fellows for the more practice-oriented engagements during the in-person week in Estonia.

During the **second week** (14—18 September, in-person), fellows will participate in expert meetings, roundtable discussions, and field visits in Tallinn and Tartu, engaging with representatives from Estonia's cybersecurity and digital governance ecosystem.

During the in-person component, fellows will also work in small groups to develop a practical capacity-building presentation on a selected cybersecurity policy topic linked to the NCSI indicators. Drawing on international good practices and their own experience, groups will deliver a short presentation with recommendations to address the identified challenges.

The programme will also include networking and social activities, such as an ice-breaker reception, hosted dinners, fireside discussions, and guided tours, fostering professional connections and peer learning among participants and speakers.

Target Audience

We welcome applications from professionals who meet the following criteria:

Tallinn
Cyber Capacity-Building
Fellowship Programme
2026

- **Background:** Junior to mid-level experts in cybersecurity, cyber diplomacy, policymaking, law enforcement, academia, civil society, or the private sector
- **Geography:** Applicants must be from the EU global partner countries
- **Experience:** Demonstrated engagement in cybersecurity-related work
- **Sectoral Representation:** A third of selected fellows is expected to come from civil society organisations working on cyber policy, advocacy, or digital rights

Application Process

To apply, applicants must complete and submit an online application form, including the following:

1. A brief **statement of purpose** (maximum 400 words) outlining the applicant's professional experience, motivation, and how the Fellowship aligns with their current work and future objectives;
2. Details of a **professional reference** from the applicant's employer, a senior official, or another relevant institution within the cybersecurity ecosystem. Applicants should provide the referee's name, position, organisation, relationship to the applicant, and contact information. No separate recommendation letter or document upload is required.

Applications will be evaluated based on merit, relevance, potential impact, and diversity considerations. Final selections will be made by a joint panel of e-Governance Academy programme organisers and the European Commission representatives.

Application Deadline: 1 July 2026

Notification of Results: 10 July 2026

To submit the application, visit **https://forms.office.com/e/Vb59R8M3dn**

Practical Information

The main venue during the in-person component of the Fellowship Programme in Tallinn will be the e-Governance Academy Events Hub (Ahtri 6, 10151 Tallinn). Time will be allocated within the programme for participants to work on the practical group assignment (capacity-building presentation), and dedicated sessions will be indicated in the programme schedule.

The organisers will cover the following participation costs for the selected Fellows:

- Round trip flights to and from Tallinn
- Accommodation during the in-person week

Global Gateway

eGA e-governance academy

- Visa fees, where applicable (reimbursed by the organisers)
- Local transportation and meals throughout the programme, including airport transfers in Tallinn

Please note that daily allowance will not be provided. Participants are responsible for arranging their own travel insurance, as well as covering any additional personal expenses or travel outside the official programme. Costs related to travel to and from the participant's local departure airport are not eligible for reimbursement.

Further Engagement Opportunities

Applicants who are not selected for this edition of the Fellowship are encouraged to remain engaged with the e-Governance Academy and consider applying to future editions of the programme. Those with more advanced professional experience in cybersecurity policymaking or cyber diplomacy may also explore opportunities to apply for the Tallinn Cyber Diplomacy Summer School. For more information about the European Commission funded **Tallinn Cyber Diplomacy Programme**, please visit www.tallinncyberdiplomacy.ee

About the Organisers

The Cyber Capacity-Building Fellowship Programme is part of an European Commission funded multi-year project under the **Global Gateway Initiative**. The Global Gateway 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 Fellowship Programme is implemented by the **e-Governance Academy** (eGA), a centre of excellence for increasing the prosperity and openness of societies through digital transformation. For over two decades, the eGA has collaborated with more than 300 organisations across 147 countries to advance digital innovation, strengthen national cybersecurity, and enhance cyber governance and cyber skills. Since 2016, eGA has developed and managed the National Cyber Security Index (NCSI) (ncsi.ega.ee) — a tool that measures countries' preparedness to prevent and mitigate cyber threats, manage cyber incidents, and strengthen national cybersecurity capacity.