

UN OEWG: Capacity-building mapping exercise – Estonia

EstDev – Estonian Centre for International Development,

- **Djibouti, Kenya, Somalia: Initiative for Digital Government and Cybersecurity in Horn of Africa countries; 01.04.2022 – 31.03.2024; 365 000€ (GIZ; ESTDEV)**

The Initiative for Digital Government and Cybersecurity in Horn of Africa Countries aims to support the governments of Djibouti, Kenya, and Somalia in strengthening e-governance and developing human-centered e-services. ESTDEV contributes to this effort by conducting digital maturity studies on each country as well as preparing roadmaps for implementing human-centered e-services. Partners: GIZ (German Development Agency), ITU (International Telecommunication Union), DIAL (Digital Impact Alliance).

- **Cyber Defense Academy support project in Moldova; €30,000.**

Aims to strengthen Moldova's Cyber Security Master's degree programs.
Funding Estonian state budget

RIA – Estonia's Information System Authority

- **EU CyberNet; 2019-2025; Funded by the EU; 9 000 000€**
 - RIA leads the EU-funded project EU CyberNet since 2019 until 2025 August. Built to bridge the expertise across the European Union, the EU CyberNet has gathered a community of 300+ cyber experts with more than 43 competence areas to develop cyber capabilities outside the EU. The experts are conducting short-term missions to train, perform or consult globally, with a focus on the Latin American and the Caribbean countries. A Regional Cyber Competence Center (LAC4) was opened in May 2022 in Santo Domingo, Dominican Republic. The total budget of the project is 9 million euros.

eGA – Estonia's e-Governance Academy

- **European Peace Facility Assistance Measure on Cyber Defence Capacity Building; 03/2022-02/2024; Funded by the EU 3 000 000€**
 - The project aims to enhance the overall resilience of Ukraine to counteract cyber threats as well as strengthen the capacities of the Ukrainian Armed Forces,

including their ability to provide services to civilians in crises or emergency situations, in particular providing support in cyber environment.

The European Union has supported the capabilities and resilience of the Ukrainian Armed Forces with the European Peace Facility (EPF) assistance measures since the beginning of Russia's war of aggression against Ukraine. The EPF enables capacity-building activities for military actors and the provision of training, equipment, and infrastructure for security purposes.

- **European Peace Facility Assistance on Cyber Defence in Moldova; 12/2022-11/2024; 09/2023 - 09/2025; Funded by the EU 3 000 000 €; 1 000 000 €**

- Moldova is currently going through a process of transition to an information society and cybersecurity has a significant influence on its stability. As a result, the EU has provided support in cyber resilience in Moldova. EU's European Peace Facility (EPF) was established to enable capacity building of military actors, and to provide training, equipment, and infrastructure for security purposes. The cyber defence component of the EPF assistance measure in Moldova will increase the ability of the Moldovan Armed Forces and the Ministry of Defence to detect intrusion to the information systems and to counter cyber-attacks.

The project covers the following main activities to achieve the goals:

- Cyber defence training and exercises
- Preparation for and delivery of cybersecurity equipment

Projects outcomes will be the improved network infrastructure and reinforced cyber defence capacities of Moldova.

- **Cybersecurity Rapid Response for Albania, Montenegro and North Macedonia; 08/2022 - 12/2023; Funded by the EU 2 600 000 €**

- A digital society with its assets and services cannot safely exist without a solid cybersecurity framework. Within the EU-supported project "Cybersecurity Rapid Response project for Albania, Montenegro and North Macedonia" eGA experts contribute to the improvement of cyber resilience in compliance with EU acquis and best practice for these beneficiaries. The primary beneficiaries

are public sector cybersecurity stakeholders in Albania, Montenegro and North Macedonia.

- The outcome of the action is strengthened governance structures and improved cybersecurity incident and risk management of Albania, Montenegro and North Macedonia
 - The project covers the following main activities to achieve the goals:
 - Providing support for the establishment of a functional governance model for cybersecurity and protection of critical infrastructure;
 - Giving advice on how to adjust the normative-legislative framework on cybersecurity;
 - Supporting the improvement of Computer Security Incident Response Teams' organisational and technical capacity;
 - Strengthening CSIRTs' professional training and community building;
 - Developing technical skills of cybersecurity experts of governmental agencies and critical service providers through technical cybersecurity exercises
-
- **Digital empowerment of the Ukrainian refugees in Estonia.** 03/2022-02/2024;
Funded by US Department of State; 236 123 USD
 - This project aspires to enable Ukrainians living in Estonia to learn about and use Estonian and Ukrainian digital solutions, satisfy their practical needs and enhance community support. We intend to recruit around 60 young digital-savvy Ukrainians in Estonia as digital envoys. They will assist over 1,000 digitally vulnerable Ukrainians in using both Estonian and Ukrainian digital e-services and solutions with the potential to raise awareness among 10,000 Ukrainians. The vision is for vulnerable Ukrainian citizens to have an improved quality of life by being skilled in using Estonian and Ukrainian e-services and digital solutions.
The project has three main objectives:
 - Ukrainian students and digitally vulnerable refugees build a stronger and more supportive community.
 - The Ukrainian digital envoys feel a sense of achievement by addressing their digital literacy needs and helping others.

- A significant number of Ukrainian citizens living in Estonia are aware of the digital transformation in Estonia and Ukraine.

The objectives will be achieved by strategic training, mentoring and awareness rising events. The core envoys will give their input to the Paide Opinion Festival and eGA's annual e-governance conference. Public presentations help raise awareness on a broader scale about the bottlenecks Ukrainians living in Estonia are facing and how the project has affected their lives.

- **Moldova Cybersecurity Rapid Assistance; 05/2022 - 05/2024; Funded by the EU** (amount not disclosed)

- The European Union introduced Rapid Assistance Project in Moldova to increase the cyber resilience of public sector organisations and key critical infrastructure sectors. Within the project, eGA experts supports national competent authorities in aligning their operations with the EU NIS Directive. To increase cyber resilience and support cybersecurity incident and risk management eGA experts:

- define the responsibilities of a governance model for cybersecurity and minimum cybersecurity baselines;
- improve cyber incident management and monitoring mechanism;
- support the development of the cybersecurity operations centre and information-sharing platform;
- develop technical skills of cybersecurity experts of governmental agencies and critical service providers
- establish communication channels and cooperation mechanisms between public and private agencies to ensure the operation and recovery of critical services and infrastructures.

The beneficiaries are the most relevant national stakeholders in the cybersecurity space in Moldova. The activities of the project are carried out by the e-Governance Academy.

- **Cybersecurity Capacity Building in the Western Balkans; 03/2023-03/2026; Funded by the EU 5 000 000€.** Partners: National Cyber and Information Security Agency of the Czech Republic (NUKIB) Center for International Legal Cooperation (CILC).

- The aim this project is to enhance the cyber resilience of the Western Balkans in compliance with EU acquis and best practices by improving cybersecurity prevention, preparedness and response of relevant public and private stakeholders in the Western Balkans countries Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia.

The action consists of four components.

- Cybersecurity governance and awareness. The activities in this component are aimed at strengthening organisational skills and mandates of public institutions on cybersecurity and improving capacities and mechanisms for cooperation.
- Legal framework, cyber norms, and international law. The activities in this component are aimed at operationalizing understanding of public institutions on EU acquis related to cybersecurity, cyber norms and international law.
- Risk and crisis management. The activities in this component are aimed at establishing and strengthening cyber risk and crisis management mechanisms.
- Operational capacities. The activities in this component are aimed at increasing operational capacities of Computer Security Incident Response Teams (CSIRTs) in cyber incident management.

- **European Peace Facility Assistance on Cyber Defence in Georgia; 05/2023 - 05/2025; 09/2023 - 09/2025; Funded by the EU 3 200 000€, 1 000 000€**

- EU's European Peace Facility (EPF) was established to enable capacity building of military actors, and to provide training, equipment, and infrastructure for security purposes. The cyber defence component of the EPF assistance measure in Georgia will enhance the cybersecurity resilience of Georgia by developing the cyber defence capability of the the Cyber Security Bureau under the Georgian Ministry of Defence and the Armed Forces of Georgia. The focus of actions is on increasing the capacity of detecting intrusions in information systems and countering cyberattacks.

The project aims to provide essential cyber software and hardware, as well as to reinforce the cyber defence capacities through trainings. The training courses will include certification courses and hands-on technical training.

Project outcomes will be the improved network infrastructure and reinforced cyber defence capacities of Georgia.

- **ENISA Framework Contract; 03/2021 - 03/2024; EU Funded 600 000€**

- Cybersecurity is an integral part of Europeans' security. The EU's democracy, economy and society depend more than ever on secure and reliable digital tools and connectivity. The needs for cybersecurity knowledge and competences exceeds the supply. The EU has to invest in building competences and talents in cybersecurity at all levels, from the non-expert to the highly skilled professional. For EU cybersecurity professionals to be efficient at tackling objectives, as well as to work in a constantly changing threat environment, there is a need of a continuous process of collecting, organising, summarising, analysing, communicating, and maintaining cybersecurity information and knowledge. Within the framework contract "Supporting activities on cybersecurity strategies, indexes and frameworks" eGA experts aim to provide support for ENISA's (European Union Agency for Cybersecurity) work throughout the years 2021 – 2024 on
 - assisting Member States to develop National Cybersecurity Strategies,
 - mapping the impact of cybersecurity by means of quantitative and qualitative indexes, and
 - developing cybersecurity taxonomies and (quantitative and qualitative) assessments of cybersecurity.

- **National Cyber Security Index 4.5; 09/2023-12/2023; Funded by EstDev 50 000 €**

- The COVID-19 pandemic accelerated the shift to online services and remote work, increasing the importance of cybersecurity. Russia's aggression towards Ukraine highlighted that cyberattacks are an integral part of modern warfare. Strengthening cyber resilience has become crucial for sustainable growth and security of many countries.

Due to that is increased the need for a reliable tool to measure and build national cyber security capacity. The National Cyber Security Index (NCSI) is perceived as a competent and influential contributor in international cyber discussions while also guiding countries to explore cyber defence capabilities and building reliable information societies. Moreover, the NCSI serves as a tool for

development aid projects that support the establishment of trustworthy digital societies in developing countries.

The NCSI assesses countries' cybersecurity levels across 12 capacity areas grouped into strategic, preventive, and responsive pillars. It includes 49 indicators to evaluate performance, with new indicators covering leadership, international law, cloud services, incident reporting, and more. The index aids in comparing countries and identifying cybersecurity collaboration opportunities based on digital development and cybersecurity indicators.

The project builds upon previous initiatives, introducing an updated methodology for the National Cyber Security Index (NCSI). eGA experts will continue managing NCSI's contact network, updating country profiles, developing the index website, and promoting the index among stakeholders.

The National Cyber Security Index (NCSI) has emerged from the projects "Shaping of Trusted Information Societies in Developing Countries" in 2016-2018, 2018-2020 and "Advancing Cybersecurity Capacities for Digital Transformation" in 2020-2022 funded by the Estonian Ministry of Foreign Affairs.