This project is funded by the European Union

Cybersecurity EAST

Project Synopsis

Project Title:	**CybersecurityEast**
Regional Scope:	**Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine**
Duration:	**27 November 2019 – 26 November 2022** (36 months, renewable)
Budget:	**EUR 3.121.600 mil** (funded by the European Union)
Implemented by:	**GFA Consulting Group (DE)** in Consortium with the E-Governance Academy Foundation (EE), Detecon International (DE), Action Global (CY) and in partnership with the German Federal Office for Information Security (DE)

Overall Objective	To develop technical and cooperation mechanisms that increase cybersecurity and preparedness against cyber-attacks, in line with the EU standards.
Purpose	The purposes of this contract are as follows: ▪ Strengthen the national cybersecurity governance and legal framework across the EaP countries, in line with the EU NIS Directive. ▪ Develop frameworks for the protection of operators of essential services (OES) and critical information infrastructure (CIIP) in the EaP countries, in line with the EU's relevant policy and legal frameworks. ▪ Increase the operational capacities for cybersecurity incidents management in the EaP countries.
Results from TOR	**I. National cybersecurity governance and legal frameworks in line with the EU NIS Directive across the EaP countries are strengthened** ▪ R1: National cybersecurity strategies, relevant legal frameworks and implementation documents are developed and tailored in approximation with the EU NIS Directive, as well as National competent authorities to oversee cybersecurity are designated. ▪ R2: Tailored approximation of the legal framework to the EU NIS Directive for the EaP Partner countries with an appropriate level of readiness and interest. ▪ R3: Increased involvement and participation of the private sector and the civil society in cybersecurity decision-making and implementation including through reinforcing public private partnerships and networks. ▪ R4: Cyber awareness (Cyber Hygiene) framework for all EaP partner countries proposed.

II. Protection frameworks of critical information infrastructure (CIIP) and operators of essential services (OES) are strengthened:

- R5: Owners and/or service providers of the CIIP and OES are identified in line with the EU NIS Directive.
- R6: Technical and organisational measures to manage the cybersecurity risks posed to the critical information infrastructure and OES developed.
- R7: Notification and information sharing frameworks on major cybersecurity incidents in critical information infrastructures developed.

III. Operational capabilities for cyber incidents and crisis management are increased:

- R8: National/governmental CSIRTs/CERTs designated and set-up, with operational capacities for incidents management created. In the EaP countries with an appropriate level of readiness and interest, set-up of functional national/governmental CSIRTs/CERTs based on EU best practice and standards, including tailored-made training programmes.
- R9: National cooperation between designated national/governmental CSIRTs/CERTs and owners/service providers of critical information infrastructure and OES on managing cybersecurity incidents ensured.
- R10: Cooperation between designated National CSIRTs/CERTs in EaP partner countries increased.
- R11: Establish a reporting, monitoring and threat assessment mechanisms for the purpose of producing national yearly evaluations on the basis of EU's best practice.
- R12: Strengthened regional and international cooperation on cyber incident-response mitigation and management, where applicable.

Contact:

Besnik Limaj, Team Leader: Besnik.Limaj@gfa-group.de

Project Webpage: https://www.gfa-group.de/cybersecurityeast

https://eufordigital.eu/discover-eu/eu4digital-improving-cyber-resilience-in-the-eastern-partnership-countries/