SENTER project

The project "Strengthening European Network Centres of Excellence in Cybercrime" (hereinafter – SENTER project, Reference No HOME/2014/ISFP/AG/7170) is funded by the European Commission under Internal Security Fund-Police 2014-2020 (ISFP).

The main goal of the project is to create a single point of Reference for EU national Cybercrime Centres of Excellence (hereinafter – CoE) and develop further the Network of national CoE into well-defined and well-functioning community.

Duration of the project: 24 months, the start date is 01/01/2016. The budget of the project: 1.976.848,89 euro.

Project partners: Mykolas Romeris University (MRU, the Coordinator, LT), Lithuanian Cybercrime Center of Excellence for Training, Research and Education (L3CE, LT), Ekonomines konsultacijos ir tyrimai (EKT, LT), Masaryk University (C4E, CZ), Katholieke Universeit Leuven (KUL, BE), French Cybercrime centre of Excellence (CECyF, FR), Tallinn University of Technologies (TUT, EE), University of Albstadt-Sigmaringen for Applied Science (UASAS, DE), International Cyber Investigation Training Academy (ICI, BL), Foundation for Research and Technology – Hellas (FORTH, GR) and Jožef Stefan Institute (JSI, SI). Associated partner: States of Jersey Police.

The target groups are:

- LEA organizations: police, prosecutors, judges,
- Relevant NGO and mediation institutions,
- Education – police colleges, universities, competence
- Certification and qualification control bodies
- Science – Universities, hubs, clusters, R&D institutions or departments
- International – EUROPOL, INTERPOL, EC3
- Intersecting domains networks - InSafe, FIU.NET

The project activities are grouped into WPs:

- WP1: Development of European Network of national Cybercrime Centres of Excellence

There is planned to create and develop European Network of national CoE (hereinafter – the Network), to define objectives of the Network and management processes, to develop an operational model and sustainability strategy for the Network, to elaborate the tools for improvement of Network efficiency such as Network identity Package, information exchange model and infrastructure and Network web portal. In order to facilitate further national CoE specialisation and deeper competence development principle, 3 special Interest Groups (IG) will be established in the Network.

- WP2: Best practices of new Coe and development of guidelines "How to Create CoE for Research Training and Education"

There is planned to accumulate and summarise the best practice from already operational CoE and based on this to develop guidelines, how to set up and manage the new CoE or improve management of existing CoE for Training, Research and Education.

- WP3: Small Islands virtual CoE development.

There is planned to develop a model for Small Islands (The States of Jersey, Guernsey, the Isle of Man and Gibraltar) virtual CoE, cybersecurity strategy, Law Enforcement competence strategy, recommendations for Small Islands virtual CoE operational model SINCERE based on the best practices and implement pilot model of Small Islands virtual CoE „SINCERE".

- WP4: Competence matrix and training programmes for Law Enforcement.

There is planned to develop the common cybercrime investigation competence skill matrix (competence map) will be defined as well as definition of process for competence development requesting. Based on this skill matrix two new training programmes for Law Enforcement will be developed, a description of the process how to identify Law Enforcement needs in new training programmes will be prepared and trainers for delivery of newly developed progarmmes will be trained. Developed training programmes will be presented at Network two annual conferences in Lithuanina and Slovenia.