Organisation logo

FIGHTING CRIME AND TERRORISM

PITCH SESSION

Horizon 2020

Organisation logo

Organisation Presentation

- **Location**: *Slovakia*

  - Support the performance of LEA;

  - National or International security analysis;

  - Continuing education in the field of security, intelligence and emergency management (developing of training contents and tools, implementation of the training, exercises, seminars, foreign internships, workshops, conferences, etc.);

  - Promotion of international LEA, intelligence and crisis management cooperation;

  - Raising public awareness related to security and emergency/crisis management (media events, publications, production and distribution of films, etc.);

  - Professional thematic consulting (consultations, risk assessment, thematic studies, audits, analyses, concepts, programmes, the setting of process management;

  - Implementation of the research and development of innovative products related to international security and emergency/crisis management (electronic services, application, etc.);

- **Experience:** *Organisation experience in collaborative projects*
- **Contact**:
  - *Name Galya Terzieva*
  - *Position Senior Expert*
  - *Email address terzieva@isemi.sk*
  - *Phone number*: **00421 / 907135897**

Targeted Topic

YOUR TARGETED TOPIC

SU-FCT03-2019	Information and data stream management to fight against (cyber)crime and terrorism

Operational Needs

List your 3 major needs

- *1 Improve investigation/intelligence tools – secured platform – communication and collaborative (live) infrastructure*
- *2 made greater use of analyses of online (open) data sources in trace/investigation process –be a step ahead before the offenders(groups)*
- *3 Enhance LEA capacity for crime scene investigation – live/nearly live forensics*

Project Idea

The technologies can offer a significant help to the law enforcement agencies both in the prevention, mitigation and neutralisation(investigation).

+ "security dashboard" for data aggregation

+ identification, analyse and understanding of trends of criminality,

+ Predictive crime mapping – anticipate criminal acts

+ Sensing "abnormal" behaviour/communication/transactions

+ robust architecture vs redundant and misleading information

Experience in the use of IT tools for analyses of criminal behaviour

- *IT staff employed*
- *Internal strategy on how to regularly analyse the virtual crime scene of sources like darknet, deep net, social media, data from public institutions, DNA – biopetrcis, border crossings, etc.*
- *Liaising with security agencies + public (critical) infrastructure*
- *Equipment*

Contribution

Optional slide featuring what you can provide to the consortium

- *Practitioner Skills*
- *Networking with other LEA and security NGOs + experts SELEC + North African + Near East Asia*
- *Skills in analyses of consortium needs*
- *Proposal preparation*
- *Contacts with SME working on detection and investigation software*