Cybersecurity a key research topic under Horizon 2020

RED-Alert & EnergyShield projects

Monica Florea

Software Imagination and Vision (SIMAVI)

Head of Unit European Projects

Monica.Florea@simavi.ro

European Research and Development projects

- SIMAVI participates as **technical partner** in over 30 Horizon 2020 projects and also as **coordinator** in 3 H2020 projects.
- SIMAVI provides services on the whole life cycle of projects:
  - ✓ Analysis of users’ requirements
  - ✓ Solution design and architecture
  - ✓ **Software development**
  - ✓ **Integration and interoperability**
  - ✓ Testing and validation
  - ✓ **Pilots deployment and end-users training**
- SIMAVI has a strong collaboration with relevant end-users from different domains (LEAs, hospitals, city municipalities, public authorities, research organizations and universities etc).

Horizon 2020 Security Projects

RED-Alert - Real-time Early Detection and Alert System for Online Terrorist Content based on Natural Language Processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing (**HORIZON 2020** - **Coordinator**); www.redalertproject.eu

EnergyShield - Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures (**HORIZON 2020 - Coordinator**); www.energy-shield.eu

ECHO **-** European network of Cybersecurity centres and competence Hub for innovation and Operations **(HORIZON 2020)** www.echonetwork.eu

MAGNETO - Multimedia analysis and correlation engine fr organized crime prevention and investigation. **(HORIZON 2020)** www.magneto-h2020.eu

CONNEXIONS - COrrelating big heterogeNeous data in a NEXt-generation Investigation and predictiOn platform for aNalysis and Simulation in mixed reality environments. **(HORIZON 2020)** www.connexions-project.eu

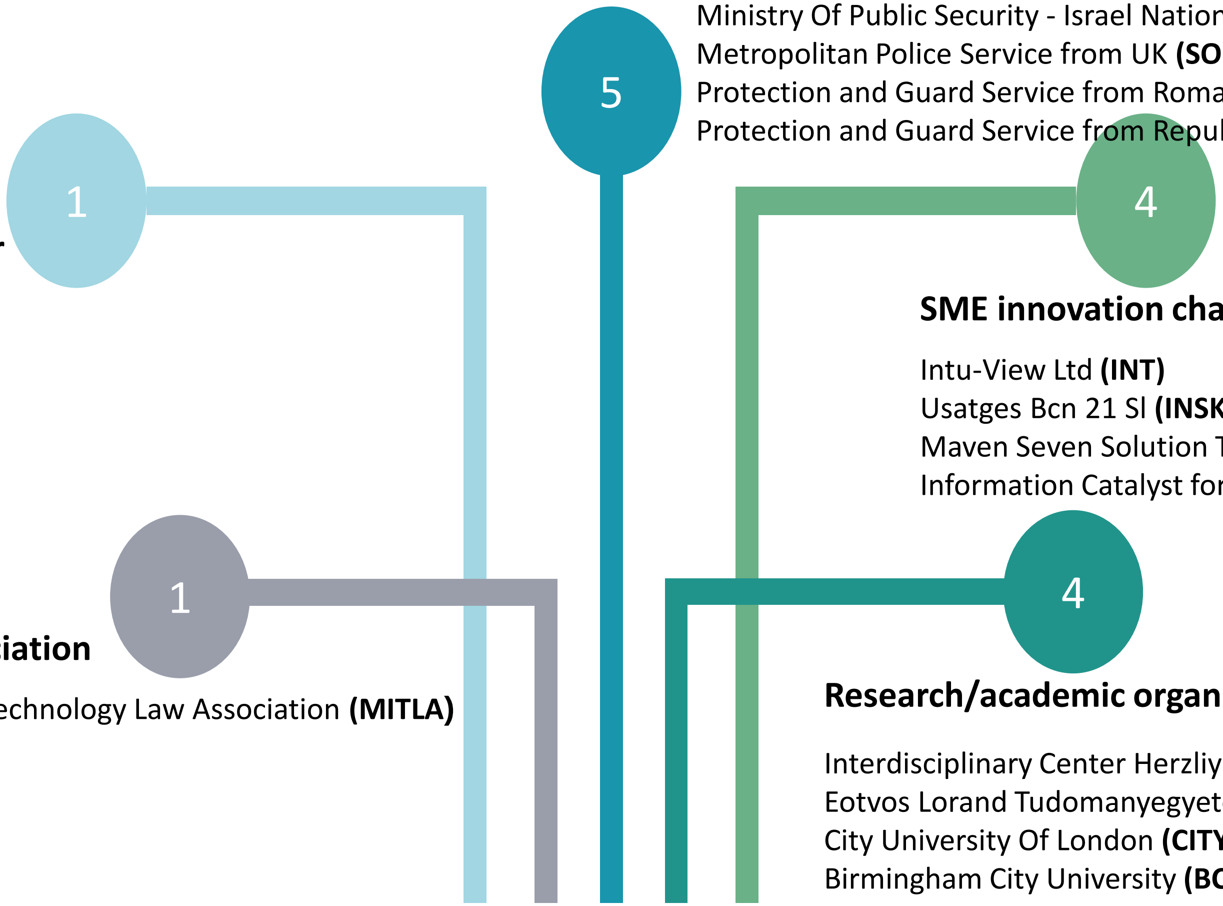
RED-Alert Project

Real-time Early Detection and Alert System for Online Terrorist Content based on Natural Language Processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing

- Project ID: 740688 (H2020, Research and Innovation Action)
- Coordinator: SIMAVI
- Start: 01-06-2017 / End: 30-09-2020
- Budget: 5,064,437 Euros
- https://redalertproject.eu/

Project consortium

15 partners from 7 countries



Law enforcement agencies

Ministerio Del Interior - Guardia Civil from Spain **(GUCI)**
Ministry Of Public Security - Israel National Police **(MOPS-INP)**
Metropolitan Police Service from UK **(SO15)**
Protection and Guard Service from Romania **(SPP)**
Protection and Guard Service from Republic of Moldova **(SPPS)**

Industrial partner

SIMAVI **(SIV)**

SME innovation champions

Intu-View Ltd **(INT)**
Usatges Bcn 21 Sl **(INSKT)**
Maven Seven Solution Technology **(MAV)**
Information Catalyst for Enterprise Ltd **(ICE)**

Regulatory association

Malta Information Technology Law Association **(MITLA)**

Research/academic organizations

Interdisciplinary Center Herzliya **(ICT)**
Eotvos Lorand Tudomanyegyetem **(ELTE)**
City University Of London **(CITY)**
Birmingham City University **(BCU)**

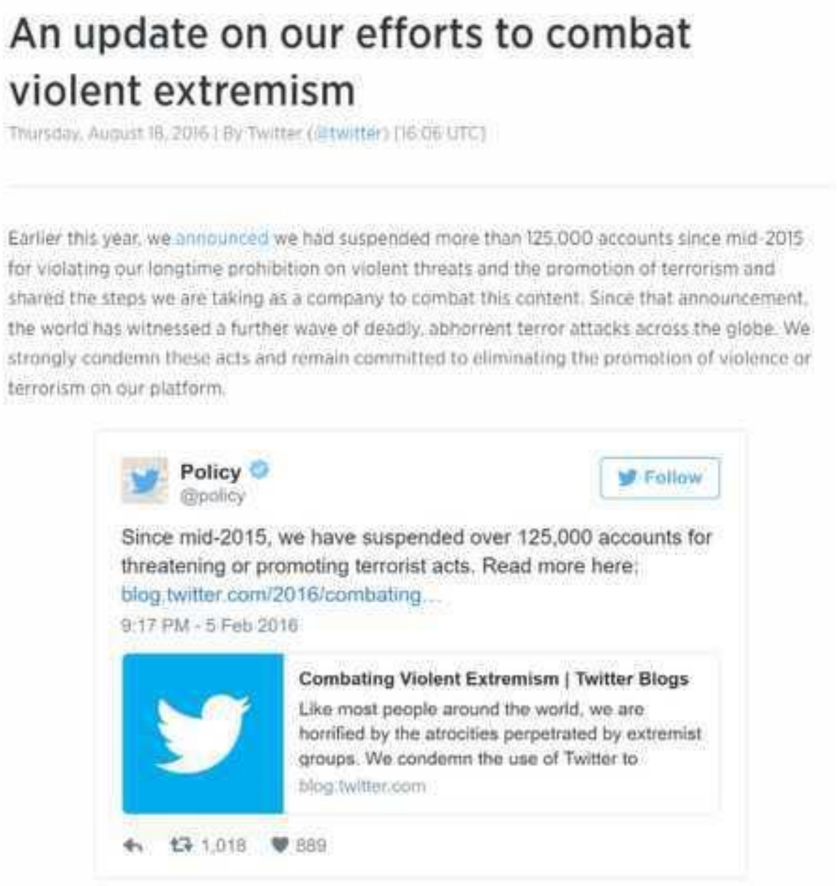
Fighting Terrorist Cyber Propaganda

Social media providers are ***determined*** to fight ***terrorist propaganda*** *on their platforms.*

There is no specific tool for identifying terrorist content on the Internet and social media ***tailored to LEAs' needs.***

LEAs must rely on proprietary spam-fighting tools, user reports and human analysis in order to detect accounts promoting terrorism.

Processing of personal data within a law enforcement context brings with it a number of ***regulatory challenges***



An update on our efforts to combat violent extremism

Thursday, August 18, 2016 | By Twitter (@twitter) [16:06 UTC]

Earlier this year, we announced we had suspended more than 125,000 accounts since mid-2015 for violating our longtime prohibition on violent threats and the promotion of terrorism and shared the steps we are taking as a company to combat this content. Since that announcement, the world has witnessed a further wave of deadly, abhorrent terror attacks across the globe. We strongly condemn these acts and remain committed to eliminating the promotion of violence or terrorism on our platform.

Policy @policy

Follow

Since mid-2015, we have suspended over 125,000 accounts for threatening or promoting terrorist acts. Read more here: blog.twitter.com/2016/combating...

9:17 PM - 5 Feb 2016

Combating Violent Extremism | Twitter Blogs

Like most people around the world, we are horrified by the atrocities perpetrated by extremist groups. We condemn the use of Twitter to

blog.twitter.com

1,018 889

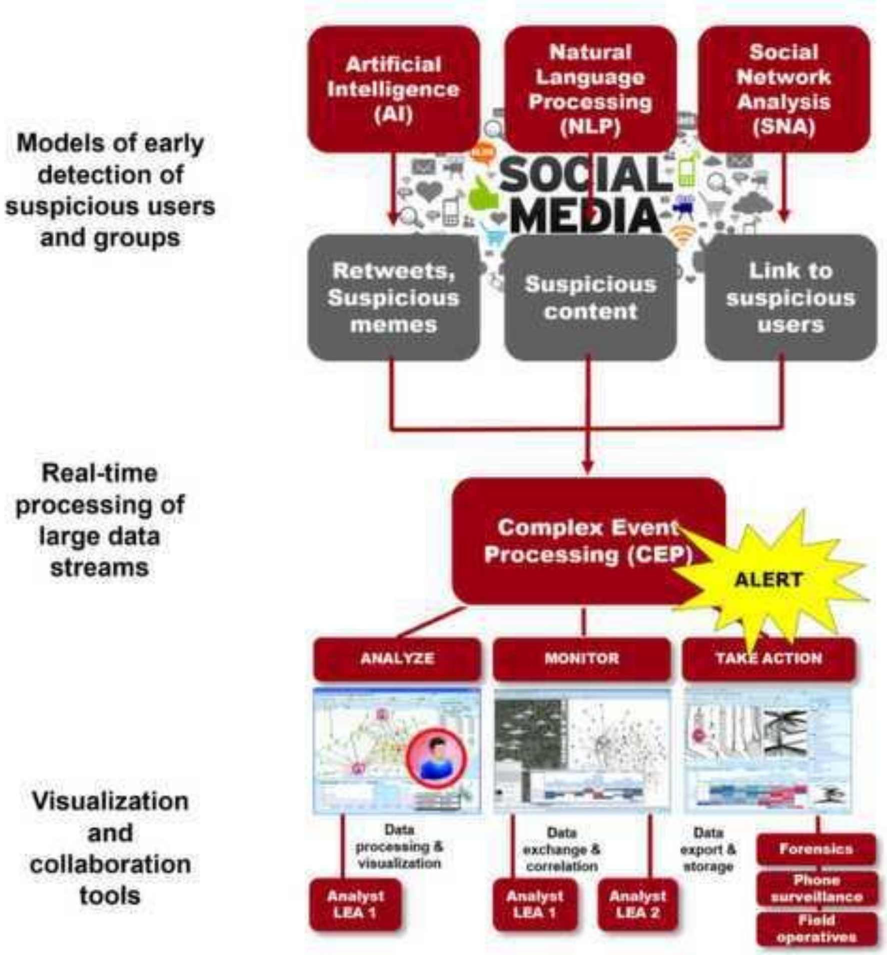
RED-Alert project objective

- **Provide a complete toolkit** for LEAs to collect, process, visualize and store online data related to terrorist groups, whether related to propaganda, fundraising, recruitment and mobilization, networking, information sharing, planning/coordination, data manipulation and misinformation.
- Cover **a wide range of social media channels**, such as Twitter, Facebook, Telegram, Instagram which are increasingly used by terrorist groups to disseminate their content.
- Allow LEAs to take **coordinated action in real-time** while **preserving the privacy of citizens**.

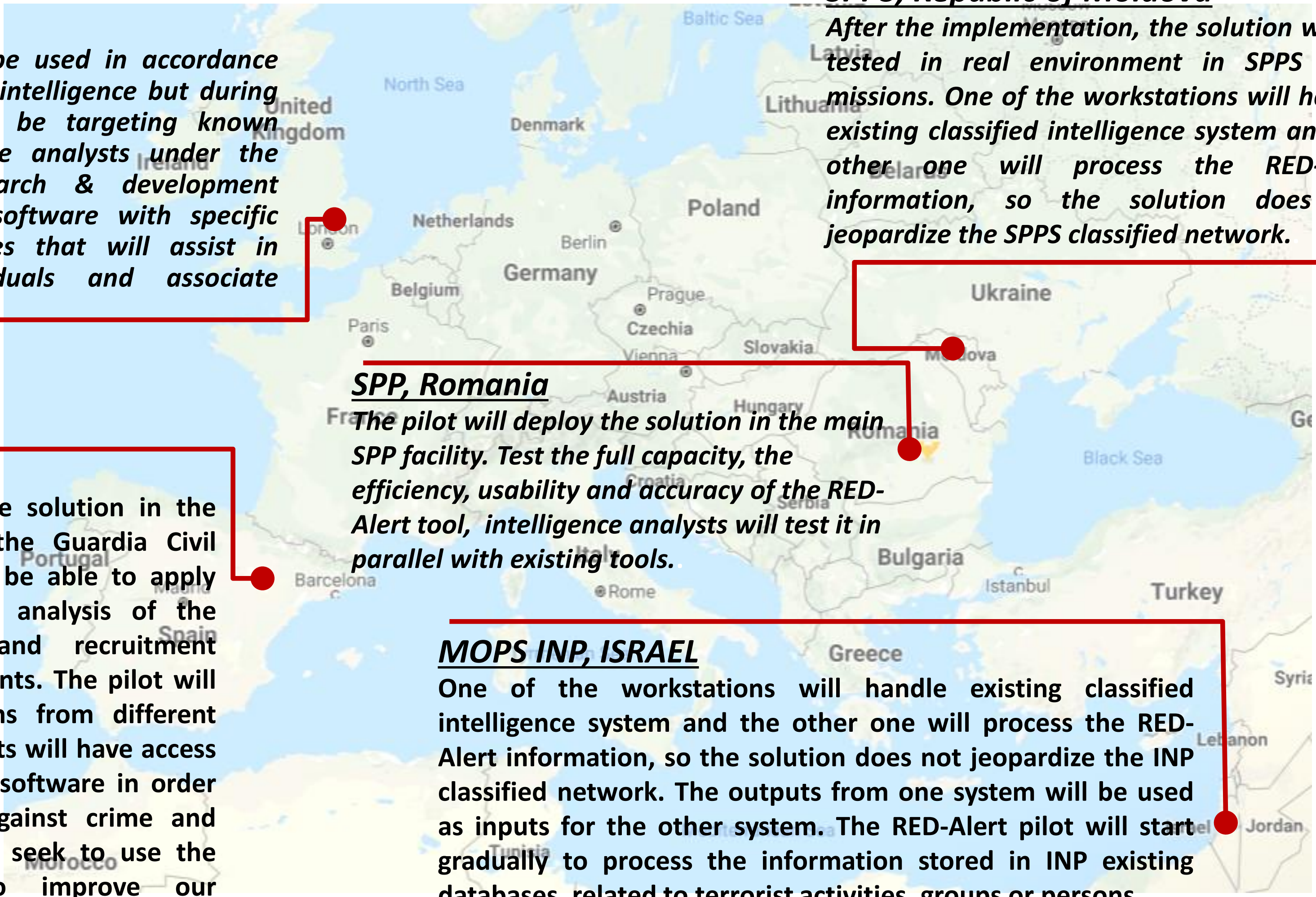
RED-Alert Innovation

- RED-Alert combines AI methods with SNA and NLP technologies to detect anomalies in content production, content nature, content spread in order to provide **early detection** of terrorist activities

- The input from AI, SNA and NLP technologies will be fed into a CEP engine to predict potential threat areas based on content production patterns, allowing the LEAs to **analyse, monitor or take action** on online terrorist content


Models of early detection of suspicious users and groups
Real-time processing of large data streams
Visualization and collaboration tools
Artificial Intelligence (AI)
Natural Language Processing (NLP)
Social Network Analysis (SNA)
SOCIAL MEDIA
Retweets, Suspicious memes
Suspicious content
Link to suspicious users
Complex Event Processing (CEP)
ALERT
ANALYZE
MONITOR
TAKE ACTION
Data processing & visualization
Data exchange & correlation
Data export & storage
Analyst LEA 1
Analyst LEA 1
Analyst LEA 2
Forensics
Phone surveillance
Field operatives

Pilots and their location



SO15, UK

RED-Alert solution will be used in accordance with RIPA on real social intelligence but during the trials, we will not be targeting known subjects of interest. The analysts under the guidance of the research & development manager will set the software with specific keywords and languages that will assist in identifying key individuals and associate networks in real time.

SPPS, Republic of Moldova

After the implementation, the solution will be tested in real environment in SPPS daily missions. One of the workstations will handle existing classified intelligence system and the other one will process the RED-Alert information, so the solution does not jeopardize the SPPS classified network.

SPP, Romania

The pilot will deploy the solution in the main SPP facility. Test the full capacity, the efficiency, usability and accuracy of the RED-Alert tool, intelligence analysts will test it in parallel with existing tools.

GUCI, Spain

The pilot will deploy the solution in the Intelligence Service of the Guardia Civil Headquarters. GUCI will be able to apply RED-Alert pilot for the analysis of the propaganda, funding and recruitment impact of terrorist elements. The pilot will encompass several teams from different GUCI units, whose analysts will have access to the RED-Alert system software in order to improve our fight against crime and terrorism. The pilot will seek to use the RED-Alert software to improve our investigations in real time.

MOPS INP, ISRAEL

One of the workstations will handle existing classified intelligence system and the other one will process the RED-Alert information, so the solution does not jeopardize the INP classified network. The outputs from one system will be used as inputs for the other system. The RED-Alert pilot will start gradually to process the information stored in INP existing databases, related to terrorist activities, groups or persons.

EnergyShield project

Type of project: H2020

Action: Innovation Action (IA)

Title: Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures (EnergyShield)

Goal:

EnergyShield captures the needs of Electrical Power and Energy System (EPES) operators and combines the latest technologies for vulnerability assessment, supervision and protection to draft a defensive toolkit.

Coordinator: SIMAVI

Project duration: 36 months; start project: 1st July 2019

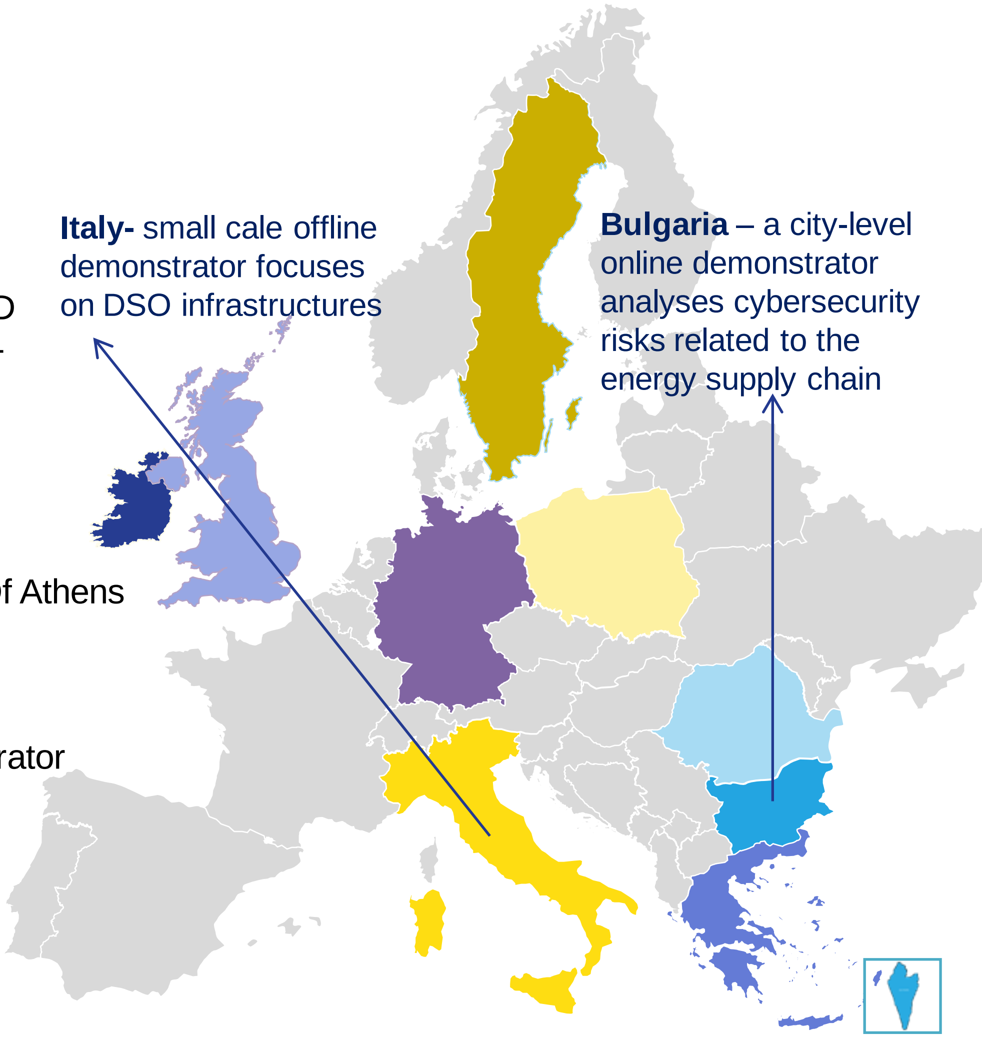
Total budget: € 7,421,437.38

Partners: 18

www.energy-shield.eu

Energy Shield Consortium and pilot

Romania:	SIMAVI
Germany:	PSI Software AG
Israeli:	SI-GA Data Security (2014) LTD L7 Defense Luxembourg SARL
Sweden:	foreseeti AB Kungliga Tekniska Hoegskolan
UK:	Tech Inspire LTD City University Of London
Ireland:	Konnekt Able Technologies
Greece:	National Technical University Of Athens
Bulgaria:	Software Company EOOD Kogen Zagore EOOD MVETS Lenishta OOD Elektroenergien Sistemen Operator EAD CEZ Distribution Bulgaria AD MIG 23 LTD DIL DIEL
Italy	IREN SPA

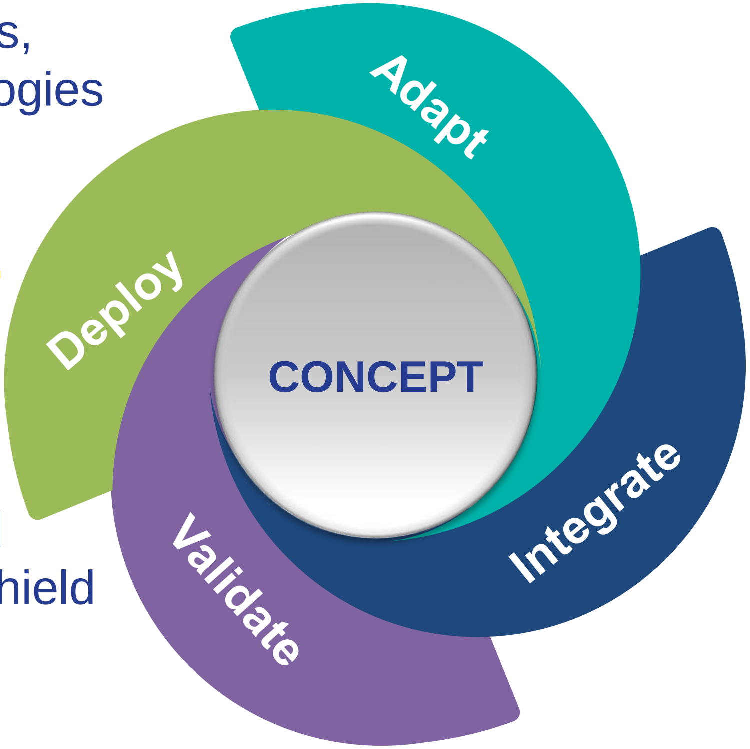


Italy- small cale offline demonstrator focuses on DSO infrastructures

Bulgaria – a city-level online demonstrator analyses cybersecurity risks related to the energy supply chain

EnergyShield - concept and objectives

Deploy best practices, guidelines, methodologies and encourage the adoption of EnergyShield results.



Adapt and improve available **tools** to support Electrical Power and Energy System (EPES) in fighting against cyber attacks.

Validate the practical value of the EnergyShield toolkit with EPES stakeholders.

Integrate the cybersecurity tools in **a holistic solution** with assessment, monitoring, protection and learning capabilities.

THE CHALLENGE

- EnergyShield project addressees small-scale and large scale disruption attack scenarios with an integrated toolkit validated in a live cyber-defense exercise

Small scale attacks

- Targeting specific organization
- Meant to prevent them from conducting business normally
- *e.g. Distributed Denial of Service, ransomware*

Large scale attacks

- Targeting the entire EPES value chain
- Meant to take down the energy supply services at regional or country level
- *e.g. malware deployment, man-in-the-middle*

EnergyShield toolkit

Vulnerability Assessment

Distributed Denial of Service Mitigation

Security Behaviour Analysis

Security Information and Event Management

Anomaly Detection

Reach out the project

Find us: www.energy-shield.eu

Subscribe for Newsletter

Follow us: @EnergyShield_

Join our LinkedIn group: EnergyShield

Contact us: EnergyShield@siveco.ro

Thank you!

Monica FLOREA
Head of Unit European Projects
Monica.Florea@simavi.ro

SIMAVI
Software Imagination & Vision