INSPECTr - 833276

Intelligence Network and Secure Platform
for Evidence Correlation and Transfer
H2020-SU-SEC-2018-2019-2020/H2020-SU-SEC-2018

INSPECTr

LEA Capacity Building as a Driver for the Adoption of European Research

https://inspectr-project.eu

Michael Whelan
INSPECTr Capacity Building Programme
inspectr@ucd.ie

CEPOL Research & Science Conference 2022
Preparing Law Enforcement for the Digital Age
Mykolas Romeris University, Vilnius, Lithuania
08-10 June 2022

This project has received funding from the European Union’s Horizon 2020
research and innovation programme under the Grant Agreement No 833276

Intelligence Network and Secure Platform for Evidence Correlation and Transfer

INSPECTr

- **Focusing on Major LEA Investigative Issues**
  - Huge volumes of data, heterogeneous strategies & outputs from tools
  - Budgetary restrictions for many agencies; training, tools, licenses, etc.
  - Legal, technical and bureaucratic obstacles to cooperation

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

Intelligence Network and Secure Platform for Evidence Correlation and Transfer

INSPECTr

- **Objectives**
  - Develop a shared intelligent platform and a novel process for gathering, analysing, prioritising and presenting key data
  - Help in the prediction, detection and management of crime in support of multiple agencies at local, national and international level
  - Reduce the complexity and the costs in law enforcement agencies to use leading edge analytical tools
  - Freely available to all LEAs

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

- **LEA partners play a central role**
  - Research and Development
  - Project Advisory Group
  - Platform Testers and Use Case developers (living labs ecosystem)

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

INSPECTr Capacity Building Programme

- **Ensures that LEAs can confidently use the system**
- Fully understand both the pitfalls and the potential of the platform
  - legal, security and ethical requirements for using disruptive and advanced technologies that:
    - provides AI assisted decision making
    - facilitates intelligence gathering from online data sources
    - redefines how evidential data is discovered in other jurisdictions and exchanged

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276

EU’s Approach to the fight against Cybercrime

- **Research and Priorities:**
  1. Adoption and update of appropriate legislation:
     - Council of Europe’s Convention on Cybercrime
     - Regulations and Directives
  2. Cross-sectoral and international cooperation:
     - European Cybercrime Centre (EC3)
     - EU Internet Forum
     - European Judicial Cybercrime Network

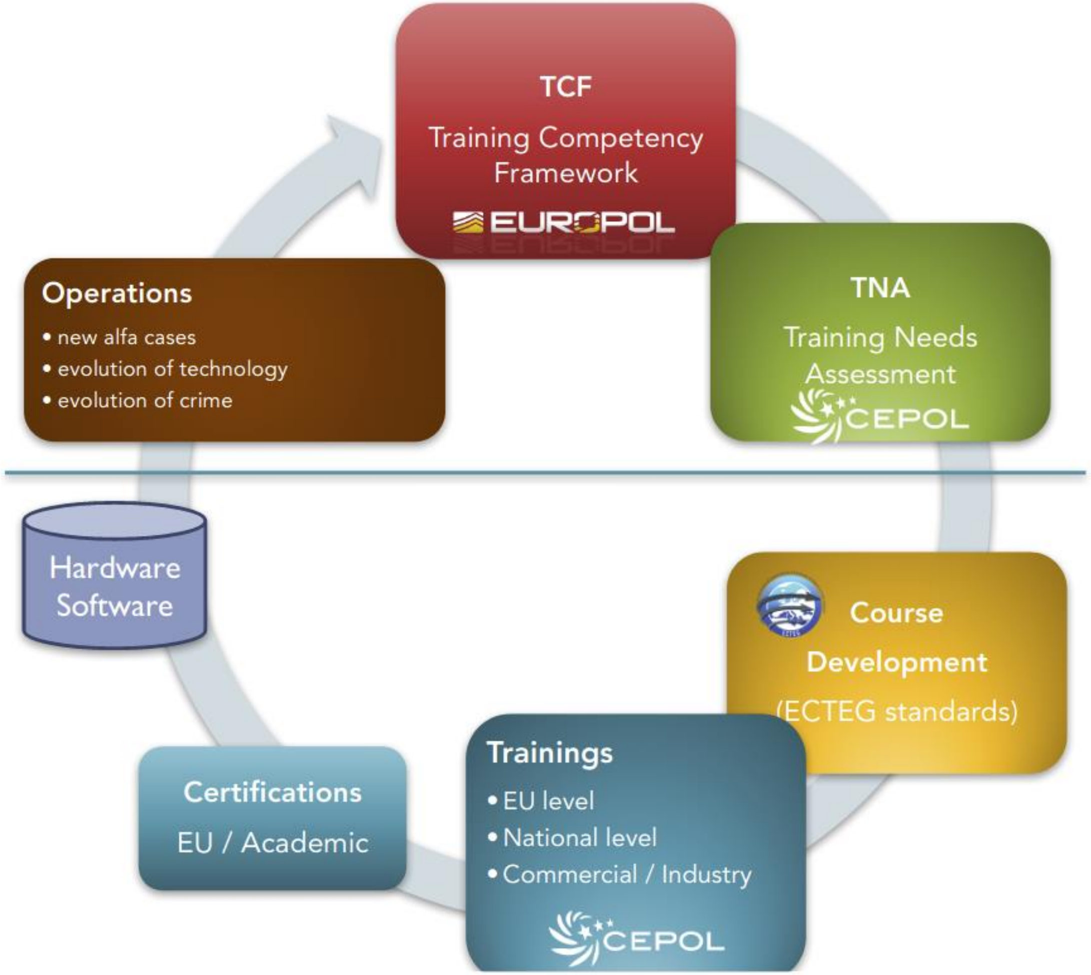
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

EU’s Approach to the fight against Cybercrime

- **Research and Priorities:**
  3. Capacity building:
     - EU Strategic Training Needs Assessment (EU STNA)
     - Internet Organised Crime Threat Assessment (IOCTA) Report
     - Training Governance Model
     - Training Competency Framework
     - Course Standards developed by ECTEG
     - Course Delivery by CEPOL

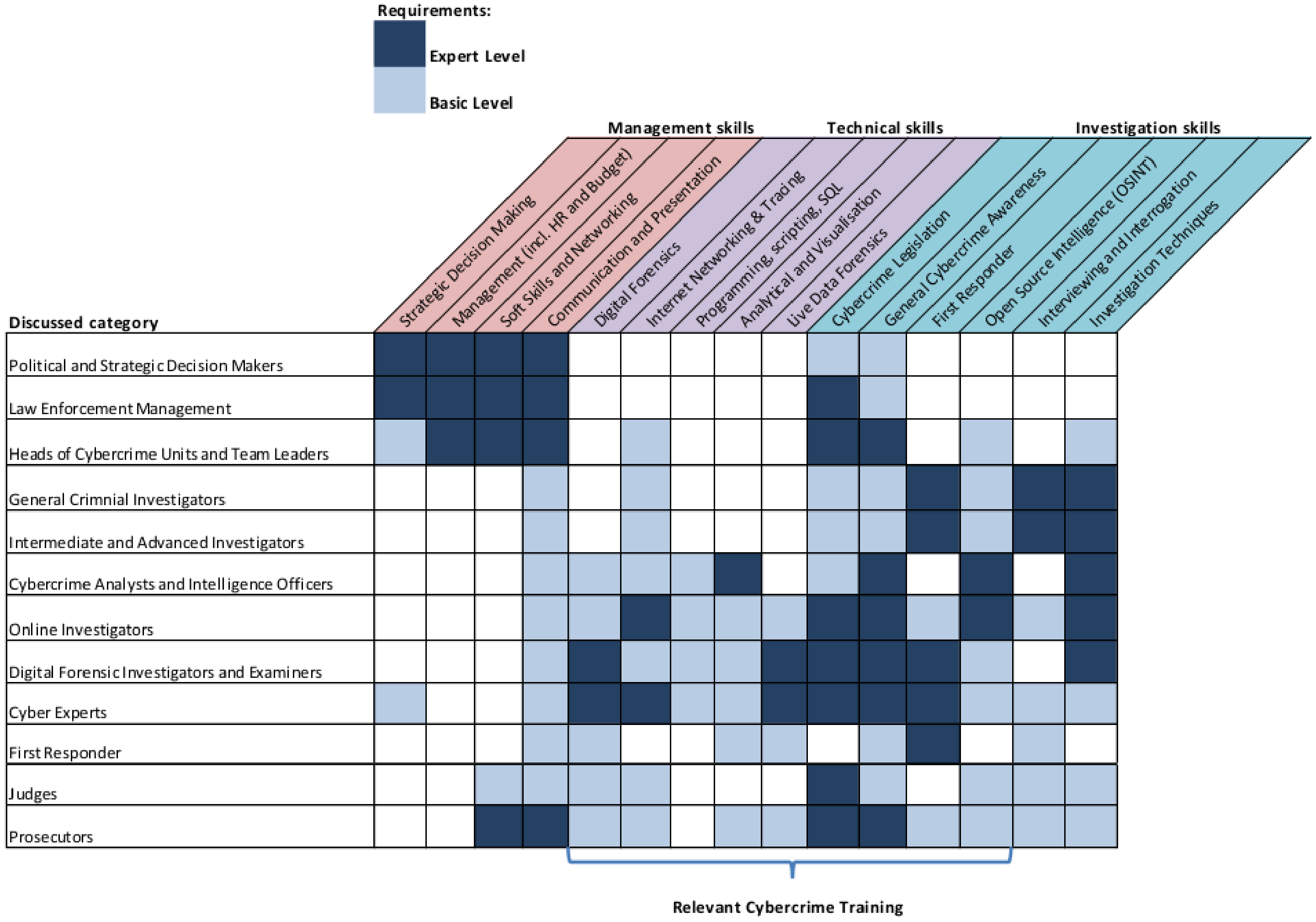
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

Training Governance Model



This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276

Training Competency Framework



Requirements:

■ Expert Level

░ Basic Level

	Management skills				Technical skills					Investigation skills					
Discussed category	Strategic Decision Making	Management (incl. HR and Budget)	Soft Skills and Networking	Communication and Presentation	Digital Forensics	Internet Networking & Tracing	Programming, scripting, SQL	Analytical and Visualisation	Live Data Forensics	Cybercrime Legislation	General Cybercrime Awareness	First Responder	Open Source Intelligence (OSINT)	Interviewing and Interrogation	Investigation Techniques
Political and Strategic Decision Makers	■	■	■	■						░	░				
Law Enforcement Management	■	■	■	■						■	░				
Heads of Cybercrime Units and Team Leaders	░	■	■	■		░				■	■		░		░
General Crimnial Investigators				░		░				░	░	■	░	■	■
Intermediate and Advanced Investigators				░		░				░	░	■	░	■	■
Cybercrime Analysts and Intelligence Officers				░	░	░	░	■		░	■		■		■
Online Investigators				░	░	■	░	░	░	■	■	░	■	░	■
Digital Forensic Investigators and Examiners				░	■	░	░	░	■	■	■	■	░		■
Cyber Experts	░			░	■	■	░	░	■	■	■	■	░	░	░
First Responder				░	░			░	░		░	■		░	
Judges			░	░	░	░				■	░		░	░	░
Prosecutors			■	■	░	░		░	░	■	■	░	░	░	░

Relevant Cybercrime Training

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

Course Development Standards by ECTEG

- Course training packages involve:
  - Decisions made with advisory group (CEPOL and EUROPOL-EC3 reprensented)
  - Use of subject matter experts
  - Creation of trainer and student manuals
  - Presentation slides and practical exercises with solutions
  - Developed using Markdown syntax, for easy translation for an international audience
  - Run at least once as pilot training

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

Course Delivery by CEPOL

- CEPOL’s approach to learning includes:
  - providing modern education methodologies such as e-learning or blended learning, which combines e-learning components with classroom or practical training
  - bringing together the latest expertise and developments in research and technology

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

INSPECTr Capacity Building TNA

- An electronic survey was used
- 15 participants from the LEA project partners
  - Each participant had to complete an informed consent before being allowed to access the survey
- All responses were pseudonymised

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

INSPECTr Capacity Building TNA

- The **first part** of the 3-part survey
- Asked the respondents about the cyber-related roles in their organisation
- The tasks referred to:
    - IT maintenance
    - forensic examination
    - monitoring the digital world
    - strategic analysis
    - operational analyses

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

INSPECTr Capacity Building TNA

- The **second part**
- Asked to share details of their best previous training involving technologies or techniques for LEA cybercrime investigation:
  - the training was internal, or developed by a third-party, such as ECTEG
  - the training was external and free by a third-party, such as CEPOL
  - the training was provided by a commercial vendor

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

INSPECTr Capacity Building TNA

- The **third and final part**
- Asked respondents about wishes for the INSPECTr training course and indicate current understanding about specific features of the INSPECTr platform, questions included:
  - their preferred method of delivery
  - how detailed the platform's manuals need to be
  - their knowledge of various topics for INSPECTr

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276

TNA Findings: Part 1

- **Need for different pathways through proposed training curricula:**
- The responses indicated that there are dedicated staff carrying out specific roles in LEA's cybercrime units:
  - 85% of respondents indicating there is at least some presence of dedicated IT staff on their team;
  - 92% of organisations have indicated there is the presence of a dedicated digital forensics member of staff on the team;
  - 84% indicate there are some staff members who are dedicated to conducting online investigations;
  - the majority of organisations have dedicated staff cybercrime analysis with 53% having dedicated staff only and 83% in total having at least one member of staff dedicated to the role;
  - finally, an extra role of a Digital Forensic Supervisor was proposed.
- Benefit: A training course can be tailored for a particular role by selecting a subset of the INSPECTr training topics that are related to knowledge and abilities needed for that role

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276

TNA Findings: Part 2

- **Replicate positive aspects from previous training experiences:**
- Majority of responses indicated that the popular preference was for:
  - training that was developed and delivered by external experts;
  - training that focused on specialised tools rather than a general overview course;
  - the delivery of the training was in-class;
  - the purpose of the training was tool specific and had instructors who gave hands-on practical-based demonstrations.
- The aim to replicate this in the proposed training courses

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

TNA Findings: Part 3

- **Focus on level of knowledge for each INSPECTr training topic, in-class training with hands-on instructor-led and practical scenario-based training:**
- According to the feedback:
  - the training format overwhelmingly preferred by the respondents would be in-class training with hands-on instructor-led and practical scenario-based training;
  - the level of knowledge of most of the respondents is very low in relation to nearly all of the INSPECTr specific topics.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

Implementing the Findings

- **Considerations:**
- Living labs conducted to test the technical developments of INSPECTr
- Continuous communication between ethics and technical partners, to highlight any such ethical and privacy issues that could arise during projects like INSPECTr

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

INSPECTr Capacity Building Programme

- **Training Curriculum**
  - Illustrates the recommendations from discussions held with the INSPECTr ethics and technical teams
  - Considered to be a fluid curriculum

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

Title	Description
Introduction	A general overview of the issues that the platform tries to address; an introduction to the platform including screenshots of the interface; an outline of additional training and pathways.
Installation and Maintenance	An explanation of hardware and networking requirements; an outline of installation steps, up to creating an admin user; an overview of system health monitoring, and updating and upgrading INSPECTr nodes; conclude with practical exercises on installation and maintenance.
Platform and User Interface	A detailed tour and focus on User Interface; an outline of the main components of a node, storage layers, gadgets, analytics, pub/sub, Blockchain, e-CODEX, etc.
Platform Administration and Configuration	An introduction to admin user tasks, such as: legal configurations for discovery and sharing, user administration - creating users and groups, tool administration - adding/restricting capabilities to groups; conclude with practical exercises on platform configuration.
External Data Ingestion	An explanation of how to configure gadgets to communicate with external storage and how to transfer data to INSPECTr storage, such as: disk images, commercial tool reports, etc.; an introduction to federated access to data using SIREN intro (as an alternative to ingestion); conclude with practical exercises on external data ingestion in INSPECTr.
Chain-of-Evidence and Chain-of-Custody	An introduction to CASE ontology and standardisation of evidence; an outline of the use of Blockchain technology for logging and tracing evidence.
Digital Forensic Tools	An outline of the use of integrated digital forensic and parsing (to CASE) commercial tool reports; conclude with practical exercises on digital forensic and Blockchain.
Open Source Intelligence (OSINT) Gathering Tools	An outline of the use of integrated OSINT gadgets, an overview of data privacy and operational security issues including ethical aspects (on data privacy, minimisation, etc.); conclude with practical exercises on OSINT.
Data Analytics and Reporting	An overview of SIREN analytics including configuration of SIREN dashboards, and federated access to external data using SIREN; an overview of INSPECTr widgets for data enriched visualisations and INSPECTr reporting; conclude with practical exercises.
AI Assisted Investigations and Proactive Policing	An outline of the use of AI tools, such as: computer vision, natural language processing, cross-case linkage, detection of criminal networks, crime forecasting, machine learning framework; ethical considerations for each aspect; conclude with practical exercises on all AI tools.
Data Discovery and Exchange	An overview of configuring and using the pub/sub for evidence discovery, configuring and using e-CODEX for evidence exchange; conclude with a joint investigation exercise.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

INSPECTr Capacity Building Programme

- **Training Pathways**

INSPECTr Topics

Roles	Introduction to the platform	Installation and maintenance	Platform and user interface	Platform administration and configuration	External data ingestion	Chain-of-evidence and Chain-of-custody	Digital forensics tools	Open source intelligence (OSINT) gathering tools	Data analytics and reporting	AI assisted investigations and proactive policing	Data discovery and exchange
IT-Administrators	■	■	▨	▨	▨	□	□	□	□	□	□
Cybercrime Investigators	▨	□	■	□	■	■	▨	▨	▨	■	■
Online Investigators	▨	□	■	□	■	■	□	■	□	■	▨
Digital Forensic Examiners	▨	□	■	□	■	■	■	□	□	■	▨
Cybercrime Analysts	▨	□	■	□	■	■	□	□	■	■	▨
Heads of Units and Team Leaders	▨	□	▨	■	□	■	□	□	□	■	▨

■ Mandatory

▨ Recommended

□ Optional

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

INSPECTr Capacity Building Programme

- **Estimated training duration for each pathway**

Pathways	Mandatory Hours of Training	Mandatory + Recommended Hours of Training
INSPECTr IT-Administrator	10	19
INSPECTr Investigators	17	29
INSPECTr Forensics	17	23
INSPECTr Intelligence	16	22
INSPECTr Analysts	16	22
INSPECTr Management	12	20

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276

INSPECTr Capacity Building Programme

- **Training Format**
  - Delivery: in-class, instructor-led demonstrations
  - Materials: slides handouts, mocked evidence, use-cases, platform user-guides
  - Evaluation: practical exercises
  - Duration: pathway dependent
- **Remote learning** or the production of videos was not considered
- Delivery of the training will target the standards set by ECTEG
  - Easier to disseminate training materials for delivery by others, a core principle for ECTEG training delivery
- In terms of **course evaluation**
  - One approach may be to engage with ECTEG-GCC (Global Cybercrime Certificate) project

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

Summary and Future Work

- The proposed training curriculum and course format will be used as the foundations for the project’s Capacity Building Programme
- The content of the training will also be subject to the findings of the living lab experiments, since LEA partners will be able to highlight any aspects of the technology that is unclear
- As per ECTEG standards, there will be the initial pilot course delivery to ensure that the training is robust and suitable for the platform’s users
- This will involve the development of the training materials and a pilot course using the proposed cybercrime investigator pathway as the target participants

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276

Thank you!

Questions?

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Grant Agreement No 833276