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

Michael Whelan

Ray Genoe

University College Dublin

Abstract

The INSPECTr project aims to produce a proof of concept that will demonstrate solutions to many of the issues faced by institutional procedures within law enforcement agencies (LEAs) for combating cybercrime. Unlike many other H2020 projects, the results of INSPECTr will be freely available to stakeholders at the end of the project, despite having a low technology readiness level. It is imperative that LEAs fully understand the legal, security and ethical requirements for using disruptive and advanced technologies, particularly with a platform that will provide AI assisted decision making, facilitate intelligence gathering from online data sources and redefine how evidential data is discovered in other jurisdictions and exchanged. However, INSPECTr will also require the support of stakeholders beyond the scope of the project, in order to drive further development and investment towards market-readiness. The development of a robust capacity building program has been included in the project to ensure that LEAs can confidently use the system and that they fully understand both the pitfalls and the potential of the platform.

During our training needs analyses, various European instruments, standards and priorities are considered, such as CEPOL's EU Strategic Training Needs Assessment, the course development standards established by ECTEG and Europol's Training Competency Framework. With this research and through consultation with internal and external stakeholders, we define the pathways of training for the INSPECTr platform in which we aim to address the various roles in European LEAs and their requirements for the effective delivery and assessment of the course. In keeping with the project's ethics-by-design approach, the training program produced by INSPECTr will have a strong emphasis on security and the fundamental rights of citizens while addressing the gaps in capabilities and training within the EU LEA community. In this paper we describe the process we apply to curriculum design, based on the findings of our research and our continued engagement with LEA and technical partners throughout the life-cycle of the project.

Keywords:

LEA Capacity Building, Training Needs Analysis, Legal, Ethical, Advanced Technologies

Introduction

According to the European Union Strategic Training Needs Assessment (EU-STNA) Report (CEPOL[1], 2019a) EU-level training should not only boost knowledge, but also allow an exchange of experiences and practices between the practitioners and contribute to building trust. The EU-STNA was developed to identify gaps in knowledge, skills and competencies and training needs. It identifies training priorities and aims at coordinating available training to prevent overlaps and duplication. It also identifies emerging law enforcement trends, such as increasing synergies and overlaps between different crime areas, as well as larger demands for cooperation between disciplines.

The undertaking of training by law enforcement personnel will not only improve their knowledge of the latest laws and legislation but also help them remain cognisant of new police tactics and evolving trends in criminal activities. For example, the ever-evolving landscape of technology provides criminals with new opportunities to commit cybercrime. Criminals are

[1] European Union Agency for Law Enforcement Training. See https://www.cepol.europa.eu/

exploiting new technologies with lightning speed, tailoring their attacks using new methods that are facilitated, enabled or amplified by the Internet (Europol[2], 2021).

Likewise, new technologies are rapidly changing the field of law enforcement in the fight against cybercrime. New automated technologies, such as artificial intelligence and predictive analytics, are being used by law enforcement to both improve efficiency and enhance safety. As the development of these technologies continues to improve and evolve, their adoption and implementation by LEAs requires proper instruction on usage, through the provision of specialised training. For example, new technology such as AI assisted intelligence gathering would have many positive aspects for police investigators but improper use could have many negative impacts on society. In addition to technical and legal obstacles barriers to the misuse of such technology, instructional training courses should also sensitise participants to the consequences of misuse.

The EU's approach to the fight against cybercrime focuses on three main areas: adoption and update of appropriate legislation; cross-sectoral and international cooperation; as well as capacity building.

Legislation: EU rules on cybercrime correspond to and build on different provisions of the Council of Europe's Convention on Cybercrime (Council of Europe, 2001). The key measures for the EU's cybercrime legal framework include:

- 2022: Proposal for a Regulation on cybersecurity requirements for products with digital elements - Cyber resilience Act (COM (22) 454 final, 2022)
- 2020: Proposal for Interim Regulation on the processing of personal and other data for the purpose of combating child sexual abuse (COM (20) 568 final, 2020)
- 2019: Directive on non-cash payment (Directive (EU) 2019/713, 2019)
- 2018: Proposals for Regulation (COM (18) 225 final, 2018) and Directive (COM (18) 226 final, 2018) facilitating cross-border access to electronic evidence for criminal investigations
- 2013: Directive on attacks against information systems (Directive 2013/40/EU, 2011)
- 2011: Directive on combating the sexual exploitation of children online and child pornography (Directive 2011/93/EU, 2011).

Using this legal framework as a foundation for an effective response to the fight against cybercrime, its measures and actions according to EU Migration and Home Affairs (2022) aim to:

- improve the prevention, investigation and prosecution of cybercrime and child sexual exploitation,
- build capacity in law enforcement and the judiciary,
- work with industry to empower and protect citizens.

Cooperation: The EU also supports cooperation frameworks amongst criminal justice actors and across sectors particularly with industry which controls a large part of information infrastructures.

Key cooperation mechanisms and structures supported by the EU include:

[2] European Union Agency for Law Enforcement Cooperation. See https://www.europol.europa.eu/

- European Cybercrime Centre[3] (EC3): set up by Europol in 2013, serves as a central hub for criminal information and intelligence and supports operations and investigations by EU Member States by offering operational analysis, coordination and technical expertise.

- EU Internet Forum[4]: established in 2015 with the aim to reach a joint, voluntary approach based on a public-private partnership with ISPs to detect and address harmful material shared online.
- European Judicial Cybercrime Network[5]: set up in 2016, facilitates sharing expertise, knowledge and best practice amongst experts from competent judicial authorities dealing with cybercrime, cyber-enabled crime and investigations in cyberspace.

The main focus of this paper will centre around the third area, **capacity building**. In the next section, we will outline the recommendations from the training governance model that was developed by various EU institutions. The remainder of the paper will be structured as follows:

- Section 3, "INSPECTr Training Needs Analysis", will describe the methodology of the training needs assessment and present a summary of our findings.
- The identified training pathways, course format and course curriculum will be discussed in Section 4, "INSPECTr Capacity Building Programme".
- Section 5, "Conclusion", will present our conclusion and future works.

Capacity Building and the Training Governance Model

In 2015, several EU agencies, namely the European Commission, Europol-EC3, ECTEG[6], CEPOL and Eurojust[7], agreed to develop a Training Governance Model (TGM) on cybercrime. The TGM was a deliverable under the EU priorities defined in the Internal Security Strategy and one of the operational actions specified for 2014 in the context of the EMPACT[8] policy cycle. The TGM intends to provide the foundations for a coordinated approach to training and education in the EU for law enforcement and the judiciary.

[3] The European Cybercrime Centre (EC3) was set up by Europol to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime. See https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[4] The EU Internet Forum (EUIF) launched by the Commission in December 2015, addresses the misuse of the internet for terrorist purposes. See https://home-affairs.ec.europa.eu/networks/european-union-internet-forum-euif_en

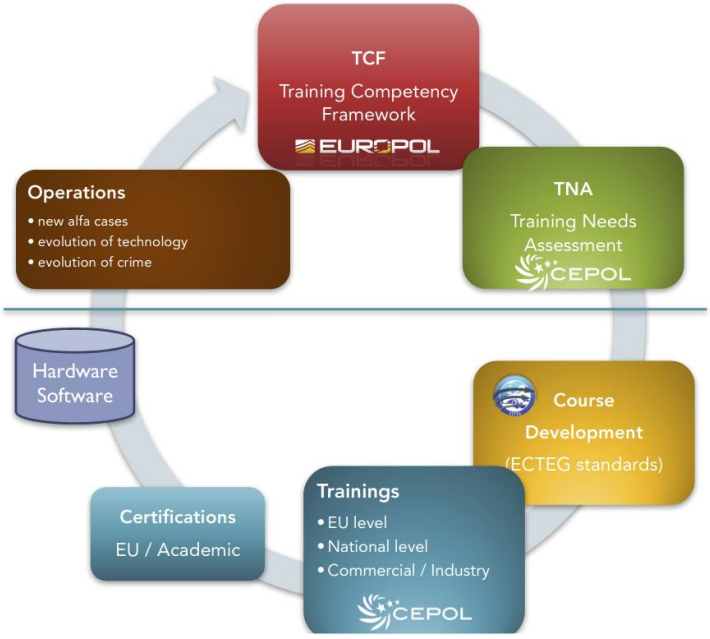
[5] The European Judicial Network in criminal matters (EJN) is a Network of national Contact Points for the facilitation of judicial cooperation in criminal matters. See https://www.ejn-crimjust.europa.eu/ejn2021/Home/EN

[6] European Cybercrime Training and Education Group (ECTEG) is an International Non Profit Association, supported by EU funding. It is composed of participants from European Union and European Economic Area Member state law enforcement agencies, international bodies, academia and private industry. See https://www.ecteg.eu/

[7] Eurojust, the European Union Agency for Criminal Justice Cooperation, is a unique hub based in The Hague, the Netherlands, where national judicial authorities work closely together to fight serious organised cross-border crime. See https://www.eurojust.europa.eu/

[8] EMPACT (European Multidisciplinary Platform Against Criminal Threats) is a security initiative driven by EU Member States to identify, prioritise and address threats posed by organised and serious international crime (EU Migration and Home Affairs, 2021).

Figure 1: TGM on cybercrime[9]



Cybercrime TGM: The Training Competency Framework

In Figure 1 the first step of the TGM is the Training Competency Framework (TCF). The aim of Europol's TCF is to identify and document the required knowledge, skills and in general the training needs of the key actors involved in combating cybercrime at EU level, focusing on both LE and the judiciary. The TCF is a living document, as the area of cybercrime is extremely dynamic, the TCF will be periodically reviewed and updated when necessary.

Figure 2: TCF on cybercrime matrix

[9] Image from ECTEG presentation to Council of Europe in 2018 (Sobusiak-Fischanaller, M. and Vandermeer, Y. 2018).

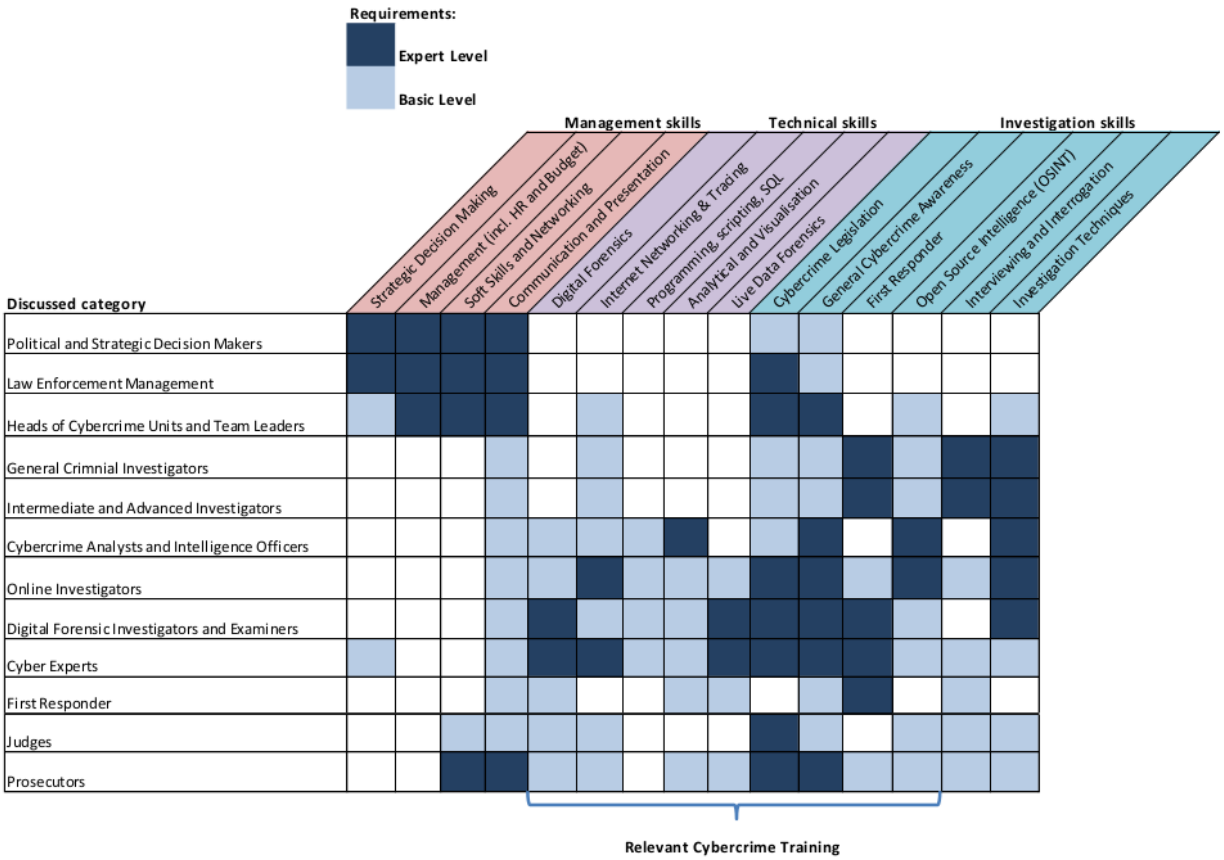


Figure 2 shows that TCF identifies ten key actors in law enforcement and two in the judiciary that are involved in the fight against cybercrime. The TCF establishes the required skills and expertise for each actor. The necessary competencies and skills described fall into three main categories – management skills, technical skills, and investigation skills. It is hoped that this standardised and harmonised description of each of the actors will ensure coherence and help avoid duplication of effort when developing training courses and educational programmes for law enforcement and the judiciary.

The strategic and operational value of the TCF can be very valuable in providing support for the coordination of organisations involved in cybercrime training and education, that will allow for a more sustainable and harmonised approach to capacity building at national and EU level. Benefits include:

- Development of a framework that specifies the skills and expertise required by the various actors involved in the fight against cybercrime
- Help minimise any overlap in the area of training and capacity building and to ensure the most effective use of budget and resources
- Define national training / education requirements
- Structure curriculum
- Help LEA to build national career paths
- Create/grow specialised units

Cybercrime TGM: Training Needs Assessment

The next step of the TGM (Figure 1) is to carry out a Training Need Analysis (TNA) based on the TCF. The analysis, as well as the consequent prioritisation of training needs and the design of the training portfolio, is a joint effort coordinated by CEPOL in cooperation the other members involved in the TGM. One such example is CEPOL's TNA for the area of cyber-attacks against

information systems (CEPOL, 2019b). The research assessed training needs against the necessary competencies law enforcement officials should have in order to perform their duties. The level of necessary competencies was defined in the TCF. The analysis provided an understanding of training needs from two perspectives:

- comparing the current level of knowledge of law enforcement officials performing different roles in investigations of cyberattacks to the level of knowledge necessary to fulfil their obligations
- identifying where there is a need for training and the dimensions of training needed such as the level, form, urgency and number of participants who would need training.

After the analysis step in the TGM, the coordination and delivery of the identified training is the responsibility of training providers such as CEPOL and ECTEG.

Cybercrime TGM: Course Development Standards

ECTEG's course development standards (ECTEG, 2022) aim to provide experience and knowledge to further enhance the coordination and support for the development and delivery of cybercrime training courses for law enforcement personnel at various levels.

The decisions to develop or update the training material of a course, are made by ECTEG members and are assisted by an advisory group that has CEPOL and Europol-EC3 permanently represented. Each course training package must follow ECTEG's course development standards which involves the use of subject matter experts and requires the creation of trainer and student manuals, presentation slides and practical exercises with solutions. In addition, courses should be developed using Markdown syntax, for easy translation for an international audience and, should be run at least once as a pilot training course for feedback and refinement.

Cybercrime TGM: Course Delivery

Within the TGM, the delivery of training is mainly led by CEPOL - who are generally responsible for the implementation of training and learning activities for law enforcement at European level. CEPOL's approach to learning (CEPOL, 2022) includes offering up-to-date, innovative training courses, bringing together the latest expertise and developments in research and technology. CEPOL provides modern education methodologies such as e-learning or blended learning, which combines e-learning components with classroom or practical training.

INSPECTr Training Needs Analysis

In light of the TCF, we wish to define pathways of training for the INSPECTr platform, which will be designed to address the various roles in European LEAs and their requirements for the effective delivery and assessment of the course. To accomplish this we carried out our own TNA.

A TNA is one of the key steps in preparing a training plan. If a TNA is not carried out there is the risk of doing too much or too little training, or missing the point completely. Conducting a thorough TNA will improve the chances of a successful training program by making informed decisions on the training composition, based on concrete data and information.

An electronic survey was used to gather the training needs for LEA wishing to use the INSPECTr platform. The **first part** of the 3-part survey asked the respondents about the cyber-related roles in their organisation. The respondents were required to indicate if there was a person or persons assigned to a specific task or was it combined with other roles. The tasks referred to were:

- setting up and maintaining the IT-infrastructure of an organisation;
- performing detailed forensic examinations of computer based digital evidence;
- monitoring the digital world and proposing new topics and cases to investigate;
- strategic analysis, researching, analysing and presenting the latest threats and providing situational overviews;
- engaging in operational analyses to find patterns, trends, hotspots and create links between live cases.

The feedback will help to define optional training pathways through INSPECTr's training curricula, which LEA can easily map to specific roles.

In the **second part** of the survey, the respondents were asked to share details of their best previous training experience, which involved technologies or techniques for LEA cybercrime investigation, whilst referring to whether:

- the training was internal and developed internally, or developed by a third-party, such as ECTEG;
- the training was external and provided for free by a third-party, such as CEPOL;
- the training was provided by a commercial vendor.

Answers to these questions will allow researchers to follow-up on specific courses that compared favourably to others.

The **third and final part** of the survey asked the respondents about what their wishes were for the INSPECTr training course and to indicate their current understanding about specific features of the INSPECTr platform. The respondents were required to answer questions on:

- their preferred method of delivery;
- how detailed the platform's manuals need to be;
- their knowledge of various topics for INSPECTr.

The responses to these questions will determine the delivery of training and the level of detail required for providing instruction on the main features of the INSPECTr platform.

The group consisted of 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, so that none of the participants could be directly identified by their responses.

TNA Findings

This section lists the key findings from the TNA. They will have a considerable influence on the proposed outputs described in the next section.

Need for different pathways through proposed training curricula: Considering the feedback for part one of the survey on LEA roles, it is clear that different pathways will be required through the training curricula of the INSPECTr platform. The survey 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.

The benefit for providing these pathways for the specific cyber-related roles, is that 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. More details on the pathways are found in next section.

Replicate positive aspects from previous training experiences: The outcome from the feedback for part two of the survey on positive previous training experiences was that the 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 will be to replicate this in the proposed training courses. Further details of the approach taken can be seen in the next section on training format.

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 for part three of the survey on training format and topics for proposed training:

- 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.

The preferred method of training delivery will be discussed in more detail in the next section on training format. The low level of knowledge on training topics is to be expected for any new product, so some basic levels of knowledge will need to be delivered, particularly with respect to the installation, configuration and usage of the platform. Further details on the contents of the training curriculum are discussed in the next section of training curriculum.

INSPECTr Capacity Building Programme

The training materials presented in this section are based on the findings of our TNA and the feedback from a number of Living Labs (European Commission, 2009) that were conducted during the execution of the project. Living Labs provide an opportunity for technical developers to discuss the direction of the product with LEA partners and receive iterative feedback through co-creation and testing cycles.

Also, another important consideration is the project's ethics-by-design and privacy-by-design approach to development of the platform from the ground up. A key part of this is sensitising the project partners to ethical and privacy issues that could arise during a project like INSPECTr, this needs to be reflected in the technical development and the training, to protect fundamental rights of citizens, and to avoid security errors, misuse, etc.

Training Curriculum

The following training curriculum, illustrates the recommendations from discussions held with the INSPECTr ethics and technical teams. It is considered to be a fluid curriculum, since it will be subject to change due to emerging technical developments, or issues encountered by LEA partners when they experiment with the system.

Including a curriculum of training during the ongoing process of project research and development is a difficult task, since the outcome of R&D tasks may require changes to be applied to the training material. However, it is important to define an early framework for the curriculum. The following is an outline of the topics we have initially proposed:

Introduction to the platform: 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[10], 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[11] 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[12] 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

[10] e-CODEX: e-Justice Communication via Online Data Exchange. See https://www.e-codex.eu/

[11] Search-based Investigative Intelligence. See https://siren.io/

[12] An international standard supporting automated combination, validation, and analysis of cyber-investigation information. See https://caseontology.org/

INSPECTr widgets for data enriched visualisations and INSPECTr reporting; conclude with practical exercises.

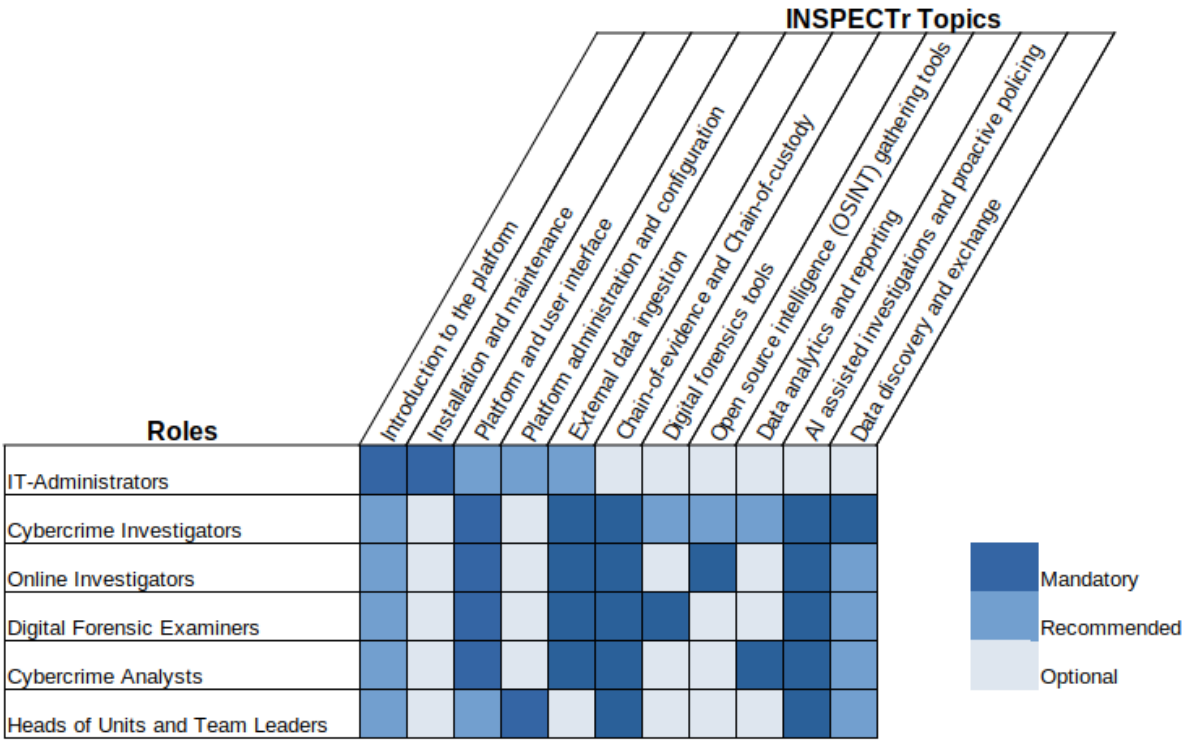
AI assisted investigations and proactive policing: An outline of the use of AI tools, such as: computer vision, natural language processing, cross-case linkage, detection of criminal networks, crime forecasting, machine learning framework; ethical considerations for each aspect; conclude with practical 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.

Training Pathways

Subsets of the topics outlined in the training curriculum section, will be chosen to define the learning pathways through the INSPECTr Training Curriculum for the specific roles in LEA's cybercrime units. The matrix in Figure 3 illustrates the proposed pathways for the chosen types of law enforcement personnel that will need to be trained to use the INSPECTr platform.

Figure 3: Pathways matrix



The proposed roles presented in Figure 3 were agreed upon after receiving the feedback from part one of the TNA survey and consulting the TCF on cybercrime seen in figure 2. Judicial training will be considered at a future stage, as the project matures (for TRL[13] 9 – System Proven in Operational Environment). Each INSPECTr topic is identified either as mandatory (blue), recommended (light blue) or optional (very light blue) to define the chosen subset for each role. The selection process, regarding how each topic is assigned for each of the roles, was agreed upon after discussions with the INSPECTr technical team.

[13] Technology Readiness Levels (TRLs) are a method for understanding the technical maturity of a technology during its acquisition phase. See https://en.wikipedia.org/wiki/Technology_readiness_level

While the estimated duration of completing all training modules would be 41 hours, the estimated duration of training each of the pathways is shown in Table 1.

Table 1: 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

Training Format

The proposed training course format will follow closely the positive aspects identified in the TNA feedback received for the previous training experiences of the respondents.

- 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 to be a requirement for the training at this stage. There are two reasons for this. The first, is that remote learning was not hugely preferred by the survey respondents, and the second is that the maturity of the platform means that videos are impractical, since the technology is subject to change. Therefore, the delivery of the training will target the standards set by ECTEG, which requires trainer and student manuals, and solutions to all exercises, to be included with the main content as presentation slides. This will make it easier to disseminate training materials for delivery by others, a core principle for ECTEG training delivery. For example, an LEA who wished to adopt the INSPECTr platform would request the training material for free and could then deliver, or seek assistance in delivering, the training. The latter may come at a cost, unless delivered by CEPOL. However, the trainer guides should assist that LEA should they wish to deliver it using in-house staff. These would also be invaluable when the platform matures and there becomes a greater need for the creation of remote learning material.

Course Evaluation

In terms of course evaluation, the maturity of the project also dictates that formal assessment cannot be considered at this time. However, after the pilot course has been completed and the final course packaged, this decision will be revisited. One approach may be to engage with

ECTEG's Global Cybercrime Certification Project[14] to determine the suitability of establishing a globally recognised certificate for each of the INSPECTr pathways described above.

Conclusion

In this paper we have described how various instruments, standards and priorities for the development of European law enforcement training, can guide the development of a robust capacity building programme for understanding emerging technologies. For example, following the different steps of the TGM, developed by key EU stakeholders, we defined the training curriculum for the INSPECTr platform, the format of the training course to deliver the curriculum and the different pathways for training different law enforcement users of the platform. We feel this is vitally important to ensure the adoption of new LEA technologies, while safeguarding the end-users from various legal, ethical or regulatory issues.

Our analysis clearly indicates that:

- tailored pathways through the training material are needed due to the number of different cyber-related roles existing in LEA's cybercrime units;
- despite the current popularity of online training, the training format overwhelmingly preferred by the respondents is in-class training with hands-on instructor-led and practical scenario-based training;
- training focused on specialised tools is preferred over general overview course material.

It is important to note that the development of the training will be an ongoing process and needs will be reflected on throughout the project, particularly after each Living Lab experiment. After the final pilot course, the training material will be packaged at the end of the project for LEA adopters of the platform. With future developments of the technology likely, the training framework will ensure that updates can be easily reflected in the capacity building program.

References

- CEPOL (2019a) *European Union-Strategic Training Needs Assessment Report 2018-2021*. Luxembourg: Publications Office of the European Union. Available from: https://op.europa.eu/en/publication-detail/-/publication/e83f9a06-c3c0-11e9-9d01-01aa75ed71a1 [Accessed on: 08 May 2022].
- CEPOL (2019b) *Operational Training Needs Analysis Cybercrime – Attacks against Information Systems*. Luxembourg: Publications Office of the European Union. Available from: https://www.cepol.europa.eu/sites/default/files/OTNA_Cybercrime_Attacks_Against_Information_Systems_2019.pdf [Accessed on: 08 May 2022].
- CEPOL (2022) *Types of Learning*. Available from: https://www.cepol.europa.eu/education-training/our-approach/types-learning [Accessed on: 08 May 2022].
- COM (18) 225 final (2018) *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:225:FIN [Accessed on: 08 May 2022].
- COM (18) 226 final (2018) *Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*. Available from:

[14] The goal of the Global Cybercrime Certification Project (ECTEG-GCC, 2022) is to create an international certification framework based on the the TCF to enable Law Enforcement Agencies and Judicial authorities to develop their knowledge and skills.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:226:FIN [Accessed on: 08 May 2022].

- COM (20) 568 final (2020) *Proposal for a Regulation Of The European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020PC0568 [Accessed on: 08 May 2022].
- COM (22) 454 final (2022) *Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.* Available from: https://ec.europa.eu/newsroom/dae/redirection/document/89543 [Accessed on: 20 September 2022].
- Council of Europe (2001) *Convention on Cybercrime 2001 (ETS No. 185)*, Available from: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 [Accessed 1 June 2022].
- Directive 2011/93/EU (2011) *Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA*. OJ L 335, p. 1–14. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093 [Accessed on: 08 May 2022].
- Directive 2013/40/EU (2013) *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*. OJ L 218, p. 8–14. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0040 [Accessed on: 08 May 2022].
- Directive (EU) 2019/713 (2019) *Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA*. OJ L 123, p. 18–29. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.123.01.0018.01.ENG [Accessed on: 08 May 2022].
- ECTEG (2022) *Course Packages*. Available from: https://www.ecteg.eu/course-packages/ [Accessed on: 08 May 2022].
- ECTEG-GCC (2022) *Global Cybercrime Certification Project*. Available from: https://www.ecteg.eu/running/gcc/ [Accessed on: 08 May 2022].
- EU Migration and Home Affairs (2021) *EMPACT fighting crime together*. Available from: https://ec.europa.eu/home-affairs/policies/law-enforcement-cooperation/operational-cooperation/empact-fighting-crime-together_en [Accessed on: 08 May 2022].
- EU Migration and Home Affairs (2022) *Cybercrime*. Available from: https://ec.europa.eu/home-affairs/cybercrime_en [Accessed on: 08 May 2022].
- European Commission (2009). Living Labs for user-driven open innovation, an overview of the Living Labs methodology, activities and achievements. European Commission, Brussels. Available from: https://op.europa.eu/en/publication-detail/-/publication/3f36ebab-4aaf-4cb0-aada-fe315a935eed [Accesses on: 10 MAy 2022].
- Europol (2021) *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Luxembourg: Publications Office of the European Union. Available from: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021#downloads [Accessed on: 08 May 2022].

- Sobusiak-Fischanaller, M. and Vandermeer, Y. (2018). *Cybercrime Training Governance Model - Cybercrime Training Competency Framework* [online]. Available from: https://rm.coe.int/3148-2-3-ecteg-16-cy-train-module/1680727f34 [accessed 25 May 2022].