# Cybercrime Training Competency Framework

09/01/2024

# CONTENTS

# Introduction

The aim of the Training Competency Framework on Cybercrime (cTCF) is to identify the required skill-sets for key actors involved in combatting cybercrime. This document serves as a framework for law enforcement authorities (LEA), as well as judiciary and academic institutions, to understand the competencies and capabilities needed to effectively tackle the ever-evolving threat of cybercrime. The framework can also be used as a basis for assessing the training needs of current and future practitioners working in the areas of cybercrime and digital investigations.

The cTCF was created following a multi-stakeholder consultation to identify the key roles and required skill sets for practitioners in the field of cybercrime. The process was supported by the European Union Agency for Law Enforcement Training (CEPOL), European Cybercrime Training and Education Group (ECTEG), Eurojust, European Judicial Cybercrime Network (EJCN), and law enforcement representatives (LE) nominated by the European Union Cybercrime Task Force (EUCTF). The renewed cTCF is part of the Commission's action plan for enhancing capacity and capabilities of law enforcement authorities in the area of digital investigations in the context of the EU Strategy to tackle Organised Crime 2021-2025.

# Approach and scope

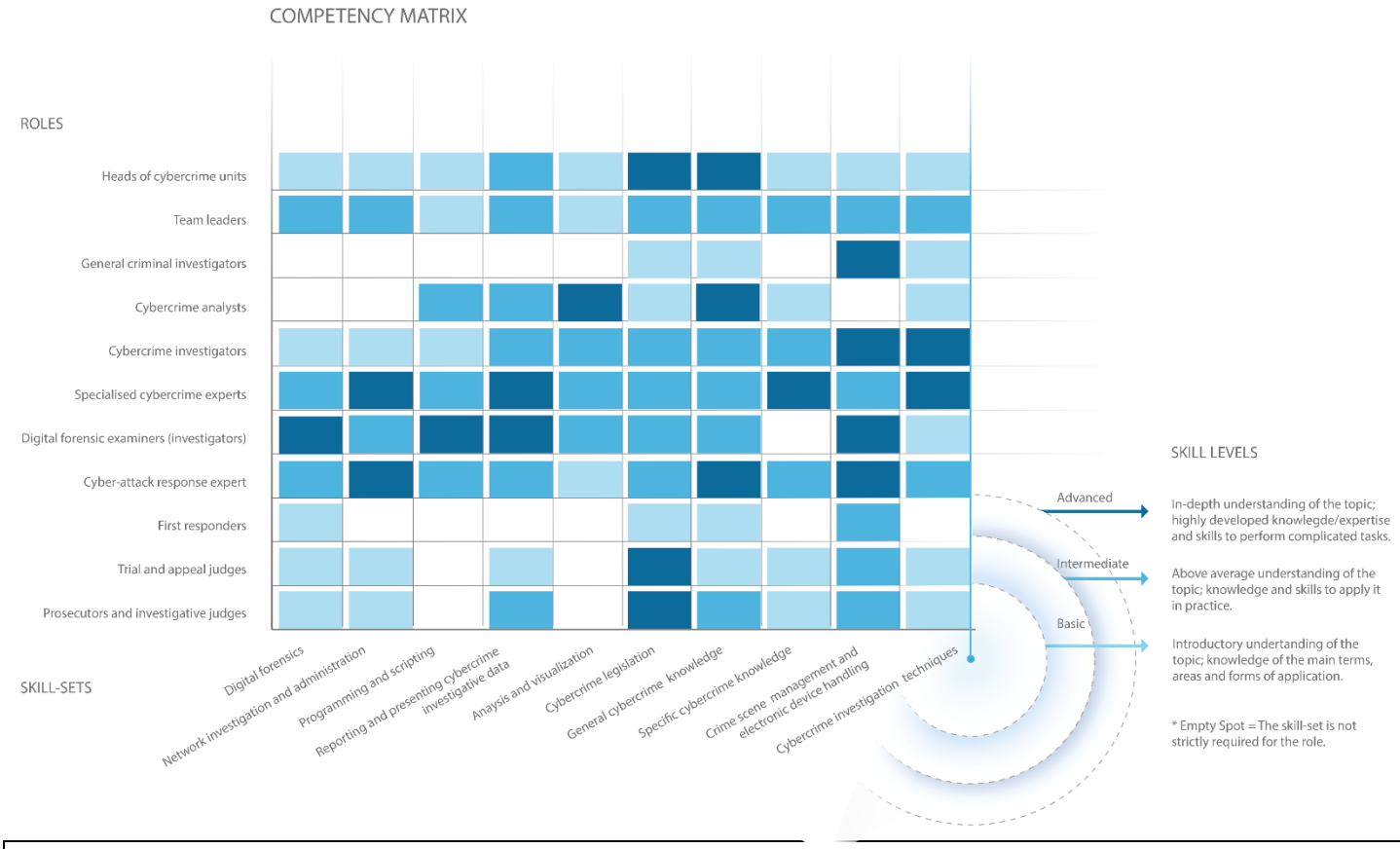
The roles and skill sets highlighted in the framework reflect the required functional competences of a law enforcement authority. The framework is not an exhaustive list of specific skills. The cTCF is not an endorsement of a specific unit structure or employee profiles. It is a description of competences that should be bolstered as part of strategic capacity building. Depending on the organisational structure and number of staff, the roles and corresponding skill sets could be combined or outsourced to a specialised unit, e.g. criminal analysis and forensics.

The scope of the framework is limited to practitioners in LEAs and the judiciary engaged in the field of cybercrime and digital investigations. The described skill sets do not reflect all the skills required to fulfil the described role, but rather pertain to skills that are unique to cybercrime investigations and the handling of digital evidence. Skills not specific to cybercrime investigations and the handling of digital evidence, e.g. general LE training, management, and soft-skills, are not included in the framework. In other words, the cTCF does not illustrate the full list of desired competencies, but instead aims to outline specialised skill-sets related to the crime area.

As mentioned previously, the skill sets consist of a non-exhaustive list of skills that are desirable in a specific role. The main purpose of the listed skills is to illustrate the general idea behind the skill set, which means that not all of them are applicable to every practitioner. For example, a forensic examiner does not have to be an expert in all areas of forensics (network, phones, operating systems, Internet of Things (IoT) devices etc.). Similarly, a cybercrime expert does not have to specialise in all areas listed under ''*specific cybercrime knowledge*'', but rather excel in specific fields.

# Framework

The training competency framework is based on the best practices, current needs, and projection of future requirements of LEA and academic institutions. The input was gathered through online questionnaires, followed by an in-person workshop and a review of the answers and results provided by the involved stakeholders (*see Introduction*). The resulting competency matrix depicts the identified roles, corresponding skill sets and desired skill levels, as seen in Graph 1. The description of the main functions and more detailed explanations of the skill sets can be found throughout the following chapters.




*Graph 1 – Cybercrime competency matrix depicting necessary key roles, skill sets and skill levels for LEA and judiciary practitioners engaged in the field of cybercrime and digital investigations.*

# Roles

## Heads of cybercrime units[1]

These professionals deal directly with cyber investigators and experts. They should take informed decisions about cybercrime cases and other complex investigations with a cybercrime component. Their role is to coordinate the structures and staff under their command, allocate resources, prioritise policing activities and identify prevention activities in the area of cybercrime to be carried out by the responsible units. They should have a detailed overview of the capacity, capabilities, and needs of the unit and provide staff with the relevant training and tools that enable or facilitate investigations and examination of evidence. Their function is also to represent the unit when dealing with external stakeholders.

Some hands-on practical experience to evaluate operational and strategic activities is recommended, as is the ability to communicate effectively with their staff and external experts. Knowledge of the English language is crucial for communication and effective relationship management within the international environment involving stakeholders from different jurisdictions and organisations such as CEPOL, Eurojust, or Europol.

## Team leaders

These professionals engage directly with cybercrime investigations, investigators and experts (cybercrime, digital forensics) within an assigned area. They should take informed decisions about cybercrime cases or in other complex investigations where cybercrime is involved. Their role is to supervise ongoing investigations, coordinate cases with senior investigators, decide on investigative measures and liaise with senior management and the judiciary.

They should have a detailed overview of the capacity, capabilities and the needs of the team for strategic planning. They should also ensure that the team has the relevant training and tools that enable or facilitate investigative activities and examination of evidence.

Practical experience to evaluate operational and strategic activities is highly recommended, as well as the ability to communicate effectively with their staff and external experts. Knowledge of the English language is important for international cooperation and the exchange of best practices.

## General criminal investigators

Investigators in other crime areas will increasingly encounter crimes facilitated by the internet and new technologies. To deal with that successfully, they should obtain a fundamental understanding of the digital world.

A key issue will be how to integrate electronic evidence into a standard crime investigation process. In general, these professionals should become more digitally aware, particularly when it comes to seizing any relevant electronic evidence at crime scenes. Their training should provide a clear list of dos and don’ts for digital seizures, handling digital material, basic legislation, and dealing with specialised colleagues.

In addition, investigators should be able to fully appreciate the amount of evidence that may be generated through open source intelligence (OSINT) and use the information effectively to complement their investigations.

## Cybercrime analysts

These professionals work in many areas: information collection, the analysis and production of actionable intelligence, strategic analysis, research, as well as presenting the latest threats and providing situational overviews. They could be engaged in operational analyses to find patterns, trends, and hotspots to create links between live cases. Analysts need to be able to process large amounts of data from different sources and

[1] *Please note that terminology can differ based on individual countries organisational set up (e.g. Units may consist of Teams in some countries while in others it they may be called Department which consist of Units). The meaning and structure is the same regardless of the terminology used.*

translate these into concise reports that clearly outline the issues in question and offer recommendations. They should disseminate the relevant knowledge within the organisation by preparing written materials and participating in strategic and operational meetings. Cybercrime analysts also need to be able to share information with wider audiences, for example in national or international reports of general interest.

## Cybercrime investigators

Law enforcement investigators specialised in Cybercrime hold extra capacity to seize electronic data and support normal investigations with cyber-related activities. They should have a more in-depth understanding of data extraction and interpretation, including in online information acquisition and seizures. They also lead cybercrime investigations, interviews and other investigative and judicial processes in cybercrime cases where the use of digital evidence is concerned. Their experience and expertise make them suitable candidates for 'training the trainers' programmes.

## Specialised cybercrime experts

These actors are law enforcement officers with specialised expertise and skills within a specific cybercrime area. They offer operational support to cybercrime investigations as well as other investigative and judicial processes in cybercrime cases. The specialisation of cyber-crime experts can range from specific forms of intelligence gathering (e.g. OSINT, Dark Web) to an in-depth understanding of specific technologies (e.g. cryptocurrencies, IoT devices) that are encountered in investigations.

Cyber-crime experts need to keep their competences up-to-date by exchanging experience, lessons learned and expertise with peers at both national and international level. They also have the skill set needed to advise authorities on potential threats and contribute to prevention activities.

## Digital forensic examiners (investigators)

These professionals identify, recover, extract, document and analyse digital evidence. They should be familiar with different operating systems, know relevant commercial and open-source tools and have scripting, programming and database querying skills. Additionally, they are required to understand forensic artefacts and data carving. They should also have a basic understanding of cryptography and be able to prepare evidence for advanced decryption tasks as well as report and present their findings. It is not necessary for them to be multi-domain experts but they should be reference points within their own area of specialisation.

They should serve as a source of technical advice for investigators requiring forensic support. These post-holders should have the skills to perform advanced forensic activities and ensure they are kept up to date.

## Cyber-attack response experts

This role includes law enforcement representatives who liaise and cooperate with other actors (Computer security incident response teams/ Computer emergency response teams, Security operations centers and related IT departments) when responding to cyber-attacks. They are responsible for initiating coercive technical countermeasures, as well as acquiring, recovering, preserving, analysing, and documenting complex (digital) traces and electronic evidence.

Their actions guarantee quality and efficiency of preserving digital evidence for investigation and prosecution in the context of cyber-attack response. This process includes international judicial cooperation from the first response to the presentation in front of judicial courts. They should have a good understanding of incident response frameworks (e.g. PICERL[2] model) and a good command of the English language and be able to effectively communicate with the involved parties, different authorities and the public.

## First responders

First responders are law enforcement officers that are the first to get in contact with potential electronic evidence. Patrol police officers, detectives, and border and tax controllers are all examples of first responders.

[2] Preparation - Identification - Containment - Eradication - Recovery - Lessons Learned

The first responder is an essential actor within the forensic process and can influence the efficiency and effectiveness of criminal investigations.

Basic knowledge of digital forensic features including live data forensics, as well as general knowledge about cybercrime. The responsibilities can entail identifying, collecting, packaging, transferring and storing devices that can contain electronic evidence at a crime scene depending on national regulation and good practices. Depending on the country, a first responder could be expected to perform urgent forensic intervention to preserve fragile or volatile electronic evidence. A first responder needs to understand which traces may be recovered by a specialised forensic examiner and how these traces may contribute to further investigation that will facilitate communication and reporting. The first responder should also be able to gather information at the crime scene and document all findings assuring the correct chain of custody. They should be able to provide basic advice to victims of cyber and cyber-enabled crimes.

### Trial and appeal judges

This category includes judges who examine cybercrime cases. Judges play a key role in the justice system, assessing the evidence and adjudicating a case.

In most EU member states, no judges currently specialise in “cybercrime”. Thus, all judges should acquire basic knowledge of cybercrime and e-evidence, which is kept up to date. One key issue will be how to integrate cyber evidence into a normal crime investigation process. These professionals should generally become more digitally aware, particularly regarding the seizure of relevant evidence at crime scenes, handling digital material, basic legislation, and dealing with specialised colleagues.

Given the increasing prominence of cyber elements in general criminal cases and the proliferation of cybercrime, basic knowledge may not suffice for a proper and just application of the law by judges. For this reason, the competency framework for judicial authorities distinguishes between general practitioners and specialists.

### Prosecutors and investigative judges

Depending on the jurisdiction, prosecutors and investigative judges may direct or oversee criminal investigations, assess the necessity, proportionality, and subsidiarity of the collection of electronic evidence, and authorise special means of investigation. Prosecutors have the prerogative to bring criminal cases before the courts and present the case in court, assessing as a first filter the evidence of a case to be presented in court. To deal with that successfully, they should obtain a basic knowledge of the digital world.

Investigative judges direct the criminal investigation and assess the necessity, proportionality and subsidiarity of the collection of electronic evidence, authorising special means of investigation.

One key issue will be integrating cyber evidence into a normal crime investigation process. These professionals should generally become more digitally aware, particularly regarding the seizure of relevant evidence at crime scenes, handling digital material, basic legislation, and dealing with specialised colleagues.

In addition, prosecutors and investigative judges should be aware of the amount of intelligence that may be generated by open-source intelligence and use the information effectively to complement their investigations.

# Skill sets

This section outlines the required skill sets and exemplifies skills they encapsulate in more detail.

### Digital forensics

Digital forensics involves the: identification, preservation, acquisition, validation, analysis, interpretation, documentation and presentation of electronic evidence. This evidence comes from digital sources and its integrity must be preserved to facilitate or further the reconstruction of crimes, or help anticipate unauthorised actions shown to be disruptive to planned operations.

This skill set consists mainly of skills in one or more of the following areas:

- Live Data Forensics
- OS Forensics (Mac, Windows, Linux, Unix)
- File System Forensics
- Mobile Forensics
- Network Forensics
- IoT Forensics
- Cloud Forensics
- Cryptography (e.g. decryption)

## Network investigation and administration

Network investigative and administrative skills pertain to knowledge of how different networks function and how to conduct investigative activities of events happening in those networks. It also includes skills related to the acquisition and analysis of traffic data to identify indicators of compromise (like command and control servers or malware beacons) that may serve as evidence for the investigation of compromised systems. These may include:

- Network administrator sets up and manages in-house networks used for data exchange and storage, malware analysis in a contained environment, configuration of network taps, etc.
- Expertise in live network data acquisition
- Network forensic and traffic data analysis
- Expertise in cyber-crime investigations and evidence retention in the context of incident responses conducted by other entities

## Programming and scripting

Programming skills are used to build information systems, whereas scripting skills mainly revolve around the automation of tasks. Scripting skills also involve executing specific functions that support investigations and data analysis as well as code or algorithm validation.

Software developers with scripting skills can support investigations through processing and visualising large amounts of data, to provide input into investigative decision-making. Programming languages like Python, JavaScript, Java, or C++, among others, can be leveraged for almost any given purpose, such as scraping data, scripting forensic acquisition commands, or creating visual dashboards.

Software developers can specialise in backend development, which deals with the acquisition, processing and management of stored data, or frontend development, which focuses on the usability and visualisation of the data. Full-stack developers are able to build complete solutions connecting a secure backend infrastructure with an intuitive user interface.

## Reporting and presenting cybercrime investigative data

Reporting in cybercrime investigations encompasses documentation, note-taking and final report writing. It can include various report types, e.g., investigative, technical reporting on findings and their interpretations, notes, journals, chain of custody, records, or others. Documentation and reporting is a transversal phase of any investigation and takes place from the crime scene to the courtroom. Any reporting aims to accurately reflect all steps taken during the investigation: the chain of custody of the evidence, the analysis and the relevant findings. Reporting needs to be executed in a structured way that will be considered factual, credible and admissible in a court of law. Hence, investigative and technical reports must be written to withstand cross-examination and replication, and prove the investigation's transparency.

Presenting investigative data means communicating data that may be technically complex to audiences without specific knowledge of cybercrime or complex technologies. This might happen during an investigation with colleagues from different units or agencies, between law enforcement and judicial authorities, or in a court proceeding. Presentation skills include synthesising information, confidently communicating and illustrating events and data as well as the ability to adapt complex technical topics to non-technical audiences.

## Analysis and visualisation

Analysis and visualisation skills consist of applying qualitative and quantitative data analysis techniques (i.e. data science) to describe, illustrate and summarise cybercrime data to find patterns, trends, and actionable knowledge. The outcomes of the analysis should be helpful for operational, tactical and strategic decision-making. Unlike investigative reporting, in this case, it is not about communicating specific data from an active investigation but about analysing data from many investigations, reliable sources and scientific research. The results may be limited to internal use but may also be published for a wider audience in national or international reports of general interest. Analysis and visualisation skills require expertise in data gathering, research design, statistical methods, visualisation best practices and being aware of ethical considerations when handling and disclosing crime data.

Some examples of advanced level skills may include expertise in analytical and visualisation tools and programming languages, machine learning, big data management and analysis and predictive policing techniques.

## Cybercrime legislation

Cybercrime legislation relates to areas and forms of different legislation governing the rights and obligations of competent authorities dealing with cyber-criminal activity. These includes:

- National legislation related to cybercrime and electronic evidence (including data processing, digital evidence admissibility, data retention, etc.)
- Privacy laws and regulations
- General Data Protection Regulation
- EU regulations on data retention
- Directives governing the cross-border exchange of digital evidence
- Procedure established for requesting data from EU countries and companies within the EU and non-EU countries and private companies
- International court rulings and precedents

## General cybercrime knowledge

General cybercrime knowledge is information related to cyber-crime that was accumulated through various sources and excludes specialised knowledge that can only be obtained with extensive and specialized training. General cyber-crime knowledge is an essential component of general overview and understanding of the cyber enabled and cyber dependent crime, cyber-crime trends, threats and *modi operandi*, electronic evidence including understanding of the cybersecurity.

## Specific cybercrime knowledge

Specific cybercrime knowledge refers to unique skills that can only be obtained with extensive and specialised training in a specific area of cybercrime and does not contain characteristics of digital forensics. This skill-set consists mainly of the skills in one or more of the following areas:

- OSINT
- Dark Web
- Blockchains and cryptocurrencies
- Intrusion analysis and incident response
- Ethical hacking
- Threat intelligence
- Malware analysis and reverse engineering

## Crime scene management & electronic evidence handling

Crime scene management and electronic evidence handling skills are relevant for any crime scene in which electronic evidence may turn up. These skills include knowledge of standards and best practices in electronic evidence identification and seizing to ensure that the evidence is not damaged or lost and can be secured for

further analysis. This includes collecting, packaging, transferring and storing devices that can contain electronic evidence.

This skill-set also includes being able to conduct on-the-scene interviews and support victims of crimes facilitated by the use of technology. On an advanced level, it can also include operational planning of action days the acquisition of volatile and non-volatile data.

## Cybercrime investigative techniques

This skill set consists of skills required for a cybercrime investigation:

- Intelligence gathering techniques
- Processing and interpreting data, cross-referencing it with LE sources
- Tracing suspects online and offline
- Online undercover work
- Cybercriminal interrogation/ questioning
- Investigation risk management.