Abstract – This document presents a comprehensive analysis of the "Europol Cybercrime Training Competency Framework 2024," a pivotal resource aimed at enhancing the capabilities of law enforcement, judiciary, and academic institutions in combating cybercrime. This analysis delves into various critical aspects of the framework, including the identification of essential skill sets for key actors involved in cybercrime mitigation, the development process of the framework, and its strategic context within the broader EU Strategy to tackle Organized Crime 2021-2025.

This document serves as a valuable resource for enhancing the preparedness and response of law enforcement and judiciary personnel to cybercrime. It underscores the importance of continuous training and capacity building in the fight against cybercrime, thereby contributing to the security and resilience of digital spaces across the European Union and beyond.

I. INTRODUCTION

The Europol Cybercrime Training Competency Framework 2024 encompasses a wide range of documents related to cybercrime training, competency frameworks, strategies, and legislation. These materials (as compilation by Europol) collectively aim to enhance the capabilities of law enforcement, judiciary, and other stakeholders in combating cybercrime effectively.

Key aspects to be explored include the framework's approach and scope, detailing the functional competences required by law enforcement authorities and the judiciary, and the flexibility and adaptability of the framework to different organizational structures. Additionally, the analysis will cover the specific roles outlined within the framework, such as heads of cybercrime units, team leaders, general criminal investigators, and specialized cybercrime experts, among others.

- **Europol Cybercrime Training Competency Framework:** outlines the necessary skill sets for various roles within law enforcement and judiciary to combat cybercrime effectively. It emphasizes the importance of digital forensics, network investigation, programming, and specific cybercrime knowledge among other skills.
- **European Union Initiatives**: Documents highlight the efforts by the European Union to strengthen cybercrime fighting capabilities through EC3 (European Cybercrime Centre) and collaborations with entities like CEPOL and ECTEG. These efforts include training, operational support, and the development of a harmonized legal framework to tackle cybercrime.
- **Global and National Strategies**: Various sources discuss the global and national strategies for cybercrime legislation and capacity building. The ITU Toolkit for Cybercrime Legislation and the National Cybercrime Strategy Guidebook by Interpol provide guidelines for developing effective cybercrime laws and strategies. These strategies emphasize the need for harmonization of laws, capacity building for criminal justice authorities, and international cooperation.
- **Training and Education**: The importance of training and education in cybercrime investigation is underscored across several sources. The National Cybercrime Training Centre (CyTrain) and the Cybercrime Investigation Body of Knowledge (CIBOK) offer specialized training and certifications for law enforcement officers and other stakeholders. These training programs cover various aspects of cybercrime investigation, including digital forensics, intelligence analysis, and management.
- **Collaboration and Information Sharing**: The need for collaboration among law enforcement agencies, private sector, academia, and international organizations is a recurring theme. Effective combat against cybercrime requires a multidisciplinary approach, sharing of best practices, and leveraging expertise from different sectors.
- **Legislation and Legal Frameworks**: Several documents discuss the challenges and recommendations for updating legal frameworks to effectively criminalize and prosecute cybercrimes. The need for laws that keep pace with technological advancements and facilitate international cooperation is highlighted.
- **Capacity Building and Resource Allocation**: The sources emphasize the need for building capacity among law enforcement and judiciary through training, provision of technical resources, and development of specialized units to handle cybercrime cases. This includes addressing gaps in skills, knowledge, and technology

II. FRAMEWORK

- **Purpose of the Framework**: The framework aims to identify the required skill sets for key actors involved in combating cybercrime. It serves as a guide for law enforcement authorities, judiciary, and academic institutions to understand the competencies needed to effectively tackle the evolving threat of cybercrime.

- **Development Process**: The framework was developed following a multi-stakeholder consultation process. This included contributions from various European bodies such as the European Union Agency for Law Enforcement Training (CEPOL), European Cybercrime Training and Education Group (ECTEG), Eurojust, European Judicial Cybercrime Network (EJCN), and representatives nominated by the European Union Cybercrime Task Force (EUCTF).
- **Strategic Context**: The renewed framework is part of the European Commission's action plan aimed at enhancing the capacity and capabilities of law enforcement authorities in digital investigations. This is aligned with the EU Strategy to tackle Organized Crime for the period 2021-2025.
- **Scope and Limitations**: The framework focuses on the unique skills pertinent to cybercrime investigations and handling of digital evidence. It does not cover all skills required for the roles described but emphasizes those specific to cybercrime. The framework is not an exhaustive list of skills nor an endorsement of a specific unit structure or employee profiles. It is intended for strategic capacity building within the organizational structures of law enforcement authorities.
- **Flexibility and Adaptation**: Depending on the organizational structure and staffing, the roles and corresponding skill sets outlined in the framework could be combined or outsourced to specialized units such as criminal analysis and forensics.
- **Functional Competences**: The framework identifies the essential functional competences required by law enforcement authorities to effectively combat cybercrime. It emphasizes the specific skills needed for cybercrime investigations and handling digital evidence, rather than general law enforcement skills.
- **Non-Exhaustive Skill List**: The framework does not provide an exhaustive list of skills but focuses on those uniquely pertinent to cybercrime investigations. This approach allows for targeted development of competencies that are most critical in the cybercrime context.
- **Strategic Capacity Building**: The framework is intended as a tool for strategic capacity building within law enforcement and judicial institutions. It aims to enhance the competencies that are crucial for the effective handling of cybercrime cases.
- **Exclusion of General Skills**: General law enforcement training, management skills, and soft skills are not included in the framework. This exclusion ensures that the framework remains focused on the specialized skills necessary for cybercrime interventions
- **Development Process**: The framework was developed through a comprehensive process that included online questionnaires, an in-person workshop, and a review of responses from involved stakeholders. This collaborative approach ensured that the framework reflects the current needs and future requirements of law enforcement and academic institutions.
- **Competency Matrix**: The competency matrix is a central element of the framework, depicting the necessary roles, skill sets, and desired skill levels for practitioners. This matrix serves as a visual guide to understanding the specific competencies required across different roles within cybercrime investigations.
- **Role Descriptions**: Detailed descriptions of the main functions and skill sets for various roles are provided throughout the framework. These roles include heads of cybercrime units, team leaders, general criminal investigators, cybercrime analysts, and specialized experts among others. Each role is tailored to address specific aspects of cybercrime and digital evidence handling.
- **Skill Sets and Levels**: The framework outlines specific skill sets required for each role and the desired levels of proficiency. These skill sets include digital forensics, network investigation, programming, and cybercrime legislation, among others. The framework emphasizes the importance of having tailored skills that are directly applicable to the challenges of cybercrime.

III. Roles

- **Heads of Cybercrime Units**: These individuals are responsible for overseeing cybercrime units, making informed decisions about cybercrime cases, coordinating resources, and prioritizing policing activities. They need to have a comprehensive understanding of the unit's capabilities and provide necessary training and tools for staff. Effective communication and relationship management skills, especially in English, are essential for interacting with international stakeholders.
- **Team Leaders**: Team leaders manage cybercrime investigations within their specific areas. They supervise ongoing investigations, coordinate with senior management, and ensure their team is equipped with the necessary training and tools. Like heads of units, they require practical experience in evaluating operational activities and strong communication skills.
- **General Criminal Investigators**: These investigators increasingly encounter cyber elements in various crimes. They need a fundamental understanding of the digital world, including how to handle electronic evidence at crime scenes and utilize open-source intelligence (OSINT) effectively.
- **Cybercrime Analysts**: Analysts are involved in collecting and analyzing data to produce actionable intelligence and strategic insights. They need to process large amounts of data from diverse sources and translate these into concise reports. Sharing information with wider audiences and participating in strategic meetings are also part of their role.

- **Cybercrime Investigators**: These are specialized investigators with a deeper understanding of data extraction and online information acquisition. They lead cybercrime investigations and are involved in training other trainers within the law enforcement community.
- **Specialized Cybercrime Experts**: These experts have specialized knowledge in specific areas of cybercrime, such as OSINT, Dark Web, cryptocurrencies, and IoT devices. They provide operational support in investigations and need to keep their skills updated through peer exchanges at national and international levels.
- **Digital Forensic Examiners (Investigators)**: These professionals focus on identifying, recovering, and analyzing digital evidence. They are familiar with various operating systems, forensic tools, and have skills in scripting and programming. They prepare evidence for advanced decryption tasks and report their findings.
- **Cyber-attack Response Experts**: These experts handle the technical response to cyber-attacks, cooperating with various stakeholders like Computer Emergency Response Teams (CERTs) and IT departments. They are responsible for preserving digital evidence and ensuring its integrity for judicial processes.
- **First Responders**: First responders are usually the initial law enforcement officers at the scene of a cyber incident. They need basic knowledge of digital forensics and cybercrime, and their responsibilities include identifying and securing electronic evidence according to national regulations and best practices.
- **Trial and Appeal Judges**: Judges dealing with cybercrime cases need to integrate cyber evidence effectively into the judicial process. They should acquire and maintain updated knowledge of cybercrime and electronic evidence.
- **Prosecutors and Investigative Judges**: These legal professionals direct criminal investigations involving cyber elements, assess the collection of electronic evidence, and present cases in court. They require a basic understanding of the digital world and the ability to use intelligence from various sources, including OSINT, to complement their investigations

IV. Skills

- **Digital Forensics**: Involves identification, preservation, acquisition, validation, analysis, interpretation, documentation, and presentation of electronic evidence from digital sources. Key areas include live data forensics, OS forensics, file system forensics, mobile forensics, network forensics, IoT forensics, cloud forensics, and cryptography.
- **Network Investigation and Administration**: Pertains to understanding network functions, conducting investigative activities within networks, and analyzing traffic data to identify indicators of compromise. Skills include network administration, live network data acquisition, network forensic and traffic data analysis, and expertise in cyber-crime investigations and evidence retention.
- **Programming and Scripting**: Utilized for building information systems and automating tasks to support investigations and data analysis. Important programming languages include Python, JavaScript, Java, and C++, among others. Skills also cover backend, frontend development, and full-stack development.
- **Reporting and Presenting Cybercrime Investigative Data**: Encompasses documentation, note-taking, and final report writing across various report types. It emphasizes the importance of structured reporting that is factual, credible, and admissible in court. Presentation skills include synthesizing information and adapting complex technical topics for non-technical audiences.
- **Analysis and Visualization**: Involves applying data analysis techniques to describe, illustrate, and summarize cybercrime data to find patterns, trends, and actionable knowledge plus data gathering, research design, statistical methods, visualization best practices, and ethical considerations in handling crime data.
- **Cybercrime Legislation**: Relates to understanding legislation governing cyber-criminal activity, including national legislation on cybercrime and electronic evidence, privacy laws, GDPR, EU regulations on data retention, and international court rulings.
- **General Cybercrime Knowledge**: Covers information related to cyber-enabled and cyber-dependent crime, cybercrime trends, threats, and modi operandi, as well as an understanding of cybersecurity.
- **Specific Cybercrime Knowledge**: Refers to unique skills obtained through specialized training in specific areas of cybercrime. Areas include OSINT, Dark Web, blockchains and cryptocurrencies, intrusion analysis and incident response, ethical hacking, threat intelligence, and malware analysis and reverse engineering.
- **Crime Scene Management & Electronic Evidence Handling**: Pertains to standards and best practices in identifying and seizing electronic evidence at crime scenes. Skills include collecting, packaging, transferring, and storing devices that may contain electronic evidence, as well as conducting on-the-scene interviews and supporting victims.
- **Cybercrime Investigative Techniques**: Consists of skills required for a cybercrime investigation, such as intelligence gathering techniques, processing and interpreting data, tracing suspects online and offline, online undercover work, cybercriminal interrogation/questioning, and investigation risk management