ENhanced AI-baSEd cybercriMe-oriented collaBorative investigation technologies and capabiLitiEs

Grant Agreement: 101168360

D2.1 Initial cybercrime landscape and investigation analysis, use cases and user requirements

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or REA. Neither the European Union nor the granting authority can be held responsible for them

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

Document Information

Deliverable number:	**D2.1**
Deliverable title:	Initial cybercrime landscape and investigation analysis, use cases and user requirements
Deliverable version:	V1.0
Work Package number:	WP2
Work Package title:	ENSEMBLE Use Cases, Requirements and New Investigation Strategies
Due date of delivery:	31st July 2025
Actual date of delivery:	29th July 2025
Dissemination level:	Public – PU
Type	Report – RE
Editor(s):	Helen Gibson (CENTRIC); Charlotte Goullion (ENSP); Charlotte Dürr (ENSP); Dimitris Kavallieros (CERTH); Ioannis Chalkias (CERTH); Darron Shannon (ULIM)
Contributor(s):	CERTH, VICOM, ENG, CFLW, IKN, CEA, BYR, TREE, UL, ULIM, RAD, ENSP, MJ, GUCI, GPI, DGPMB, CYberP, CENTRIC.
Reviewer(s):	Mark van Staalduinen (CFLW); Marco San Biagio (ENG)
Project name:	ENhanced AI-baSEd cybercriMe-oriented collaBorative investigation technologies and capabiLitiEs
Project Acronym	ENSEMBLE
Rights:	ENSEMBLE Consortium

Document history

Version	Date	Beneficiary	Description
0.1	15/04/2025	CENTRIC	ToC
0.2	06/06/2025	CENTRIC + ENSP	Initial version of cybercrime landscape, methodology
0.2	10/07/2025	CENTRIC, ENSP, CERTH, ULIM	Version 0.2 inclusion of summary of use cases and use case scenarios
0.3	21/07/2025	CENTRIC + ENSP	Version 0.3 – inclusion of summary of UR requirements section
0.4	24/07/2025	CERTH	Security Review by PSO / SAB
0.5	27/07/2025	CENTRIC, CLFW, ENG	Update to include review feedback
1.0	29/07/2025	CENTRIC, CERTH	Final version

Executive Summary

Technological advancements create opportunities for sophisticated cybercrimes that, through innovative tactics and techniques, pose serious security and financial risks to the EU and beyond. ENSEMBLE aims to combat cross-border cybercrime by utilising advanced AI-based technology, multi-stakeholder investigation processes, training, and awareness initiatives. The project focuses on detecting and preventing ransomware, cyber fraud, data theft, extortion, unauthorised access, and crypto-jacking. In response to these challenges, ENSEMBLE will develop an AI-based investigation toolbox to assist police authorities in detecting, extracting, processing, and analysing online information relevant to cybercrime activities.

For ENSEMBLE to effectively address these challenges, it is essential to have an up-to-date picture of the current state of cybercrime within Europe, the key challenges faced by LEAs, and their requirements to enhance the fight against cybercrime, both at the wider European level and in the direct operational units. In this report we find through analysis of the cybercrime landscape in Europe, that cybercrime continues to be on the rise understanding the scope and scale of this rise is hampered still by widely differently reporting practices across Europe and limited discussion not only on how many cybercrimes have occurred, but how effective law enforcement are at investigating them, overall and in comparison to other crimes. Recent years have clearly seen extensive investment into understanding and improving the cybercrime investigation process, providing clearer structures for the organisation of units, training pathways and access to data, tools and software. However, this still appears a fragmented landscape, where investigations can be carried out between and within multiple organisations (i.e., law enforcement agencies, cybersecurity companies, the victims, computer emergency response teams, financial institutions, and others). This also necessitates a vision where better sharing of information can impact the investigation landscape drastically. In this deliverable, we consider individual processes for investigating cybercrime on the dark web, through OSINT, networks, involving cryptocurrencies, third-party services, digital forensics through malware analysis, cyber threat intelligence, and the role for chain of custody, decision support, reporting and visualisation.

Separately, as a bottom-up process, it is important to consider how investigators view the cybercrime situation from the ground, in the operational setting. Therefore, in parallel, ENSEMBLE set about working with its end-user community, understanding the landscape of cybercrime investigation in the individual countries (France, Spain, Moldova, Romania and Portugal). Through a detailed user survey, ENSEMBLE was able to elicit key gaps and needs from investigators in relation to the types of cybercrime they experience, the tools they use and the legal and procedural challenges they face. Such insights directly informed the further development and enhancement of the proposed use cases within ENSEMBLE, each divided into multiple scenarios. Through a user-centric approach, ENSEMBLE researchers, end-users and technology providers worked together to deliver seven different scenarios representative of the cybercrime landscape today.

- **PUC1 – Ransomware**
  - Scenario 1: Small-scale attack of ransomware with one attacker and one victim
  - Scenario 2: Large-scale ransomware attack with approximately 20 attackers and 50 victims (Ransomware-as-a-Service)
- **PUC2 – Cyber fraud and data theft**

- Scenario 1: Data theft via watering hole attack
- Scenario 2: Data theft via fake registration form
- Scenario 3: Financial fraud

- **PUC3 – Data theft from unauthorised access**
  - Scenario 1: Data theft of multimedia to be sold on the darkweb and exploitation of system resources with crypto-jacking
  - Scenario 2: Data theft for extortion

The definition of these scenarios led to the developed of an extensive list of user requirements, mapped to ENSEMBLE's tools, and with a clear understanding of the data requirements and the needs of operational law enforcement.

The scenarios and requirements will continue as living documents throughout the project, adapting to the updated cybercrime landscape and the needs of practitioners as it continues to evolve over the coming years. The next stages include in-depth interviews with investigators, preparation of the technical requirements in line with the user requirements, and updates according to the planned piloting activities to occur next year.

Contents

Table of Figures

Table of Tables

Acronyms & Abbreviations

Term	Description
AI	Artificial Intelligence
AML	Anti Money Laundering
APP	Authorised Professional Practice
BEC	Business Email Compromise
BSI	Basic Subscriber Information
C2 / C&C	Command and Control
CCPE	Consultative Council of European Prosecutors
CEO	Chief Executive Officer
CEPOL	European Union Agency for Law Enforcement Training
CERT	Computer Emergency Response Team
CoE	Council of Europe
CPS	Crown Prosecution Service
CSAM	Child Sexual Exploitation Material
CSIRT	Computer Security Incident Response Team
CTCF	Cybercrime Training Competency Framework
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial of Service
DF	Digital Forensics
DIICOT	Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism
DGA	Data Governance Act
EC3	European Cybercrime Centre
ECHR	European Convention on Human Rights
ECTEG	European Cybercrime Training and Education Group
EJTN	European Judicial Training Network
ENISA	European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data Protection Regulation

IAB	Initial Access Brokers
IDS	Intrusion Detection System
IoCs	Indicators of Compromise
IOCTA	Internet Organised Crime Threat Assessment
KYC	Know Your Customer
LEA	Law Enforcement Agency
LED	Law Enforcement Directive
LLMs	Large Language Models
MISP	Malware Information Sharing Platform
MLAT	Mutual Legal Assistance Treaty
MS	Member State
NCSC	National Cyber Security Centre
NICCS	National Initiative for Cybersecurity Careers and Studies
OPSEC	Operation Security
OSCE	Organisation for Security and Cooperation in Europe
OSP	Online Service Provider
OTNA	Operational Training Needs Assessment
OSINT	Open Source Intelligence
PAP	Permissible Actions Protocol
SME	Small and medium-sized businesses
SOP	Standard Operating Procedure
TLP	Traffic Light Protocol
TTPs	Tactics, Techniques and Procedures
UNODC	United Nations Office on Drugs and Crime
VASP	Virtual Asset Service Provider
VAWG	Violence against women and girls

1 Introduction

Technological advancements create opportunities for sophisticated cybercrimes that, through innovative tactics and techniques, pose serious security and financial risks to the EU and beyond. ENSEMBLE aims to combat cross-border cybercrime by utilising advanced AI-based technology, multi-stakeholder investigation processes, training, and awareness initiatives. The project focuses on detecting and preventing ransomware, cyber fraud, data theft, extortion, unauthorised access, and crypto-jacking. In response to these challenges, it will develop an AI-based investigation toolbox to assist police authorities in detecting, extracting, processing, and analysing online information relevant to cybercrime activities.

For ENSEMBLE to effectively address these challenges, it is essential to have an up-to-date picture of the current state of cybercrime within Europe, the key challenges faced by LEAs, and their requirements to enhance the fight against cybercrime. This deliverable combines the results of two of the first streams of work within ENSEMBLE – an overview of the current cybercrime landscape from a broad perspective and the explicit scenarios and requirements faced by the cybercrime units directly engaged in the project. This is the first of two deliverables addressing these workstreams, with further development and refinement continuing throughout the project to ensure ENSEMBLE accurately addresses the rapidly changing cybercrime environment and provides the necessary value to law enforcement. The next version of the deliverable will be submitted at M26 of the project (December 2026), with continuous improvements and updates in the intervening period in line with the project's activities.

1.1 Relation to other tasks and deliverables

This deliverable is related to the following other ENSEMBLE tasks and deliverables:

Relation with other deliverables:

Deliverable Number	Deliverable Title	Relation (Input/Output)
D2.2	Initial cybercrime landscape and investigation analysis, use cases and user requirements (full version).	The full version of this deliverable including the restricted content related to the user survey, scenarios and user requirements.
D2.3	Final cybercrime landscape and investigation analysis, use cases and user requirements.	The second iteration of the public version of this deliverable.
D2.4	Final cybercrime landscape and investigation analysis, use cases and user requirements (full version).	The second iteration of the restricted deliverable containing the updates to the user requirements, scenarios and further research on the cybercrime landscape

D2.5	ENSEMBLE cybercrime investigation processes.	Report on the future of cybercrime investigation in line with the activities of ENSEMBLE, building on the findings of this deliverable
D2.6	ENSEMBLE legal and ethical framework.	Legal and ethical framework that supports ENSEMBLE's proposed development and solutions.
D5.1	ENSEMBLE toolbox architecture and system requirements.	Utilising the output of this deliverable to support the design of the ENSEMBLE architecture
D6.1	Initial end-user training, pilot demonstration, and evaluation.	Use cases and requirements inform the preparation of the first piloting activities

Table 1: Table of related deliverables

Relation with tasks:

Task Number	Task Title	Relation (Input/Output)
T2.1	Identification and analysis of International and European best practices of cybercrime investigation methodologies	Informs the content in Section 2 and Section 3 of this deliverable
T2.2	User centric creation, analysis, and definition of use cases and requirements	Informs the content in Section 4, 5 and 6 of this deliverable.
T2.3	The road ahead: new strategies and investigation processes	This task will use the outcomes of this deliverable to help identify the gaps in cybercrime investigation and propose future approaches
T2.4	Legal and ethical framework	This task supports the legal and ethical investigation of cybercrime
T5.5	Technical requirements specification and toolbox architecture d	The technical requirements and specification are informed by this deliverable
T6.1	Pilot and training framework	The pilots are informed by the use case scenarios and user requirements developed in this deliverable.

Table 2: Table of related tasks

1.2 Structure of the deliverable

This deliverable combines the results of two tasks under WP2 ENSEMBLE Use Cases, Requirements and New Investigation Strategies – T2.1 Identification and analysis of International and European best practices of cybercrime investigation methodologies – led by CENTRIC; and T2.2 User-centric creation, analysis, and definition of use cases and requirements led by ENSP. This deliverable is divided into two versions – this the public version (D2.1) and D2.2, the full version. The structure is the same for both deliverables, but the full version contains the detailed results of the end-user survey, use cases and user requirements. The overall structure follows like this,

- Section 2 - Overview of cybercrime in Europe in 2025 – this section discusses current classifications of cybercrime and relevant cybercrime investigation statistics.
- Section 3 – this section describes the current information about the cybercrime investigation practices in the public domain and makes recommendations on future best practices.
- Section 4 - ENSEMBLE user-centric methodology – this section describes the process undertaken by ENSEMBLE to develop the use cases and elicit the first version of the user requirements.
- Section 5 - Analysis of end-users and practitioners' needs – this section provides a brief summary of the survey undertaken with the ENSEMBLE end users to understand their current cybercrime investigation operating environment.
- Section 6 – Use Case Development – this section describes the development and providers a public summary of first version of the ENSEMBLE use-cases
- Section 7 – User Requirements this section providers a summary of the user requirements as developed within ENSEMBLE.
- Section 8 – this deliverable is first of two deliverables for T2.1 and T2.2, this section describes the proposed activities, refinement and further development for ENSEMBLE over the next 18 months.

2 Overview of cybercrime in Europe in 2025

2.1 Defining cybercrime

The prevalence of cybercrime in Europe continues to grow, fuelled by our reliance on digital infrastructure, the increase in digital devices, and the amount of data stored and accessible online. This large attack surface presents numerous opportunities for criminals to initiate and conduct cyber-related crimes. Traditionally, cybercrime can be categorised as cyber–dependent or cyber-enabled. Cyber-dependent crimes are defined as "any crime that can only be committed using computers, computer networks, or other forms of information and communication technology" [1]. Conversely, cyber-enabled crimes are traditional crimes that are facilitated, enhanced or scaled through the use of digital technology. In practice, the complexity of the cybercrime landscape means that many crimes have a cyber-enabled element, and many cyber-dependent crimes also exhibit features of cyber-enabled crime [2]. Therefore, nowadays, cybercrime investigators and investigations must adopt strategies and practices that encompass multiple investigative modalities and combine them effectively. However, the lack of precise definitions of cybercrime can cause issues for law enforcement and victims. The challenges that emerge from this lack of harmonisation around definitions and the cascading effects they cause across the justice system have been extensively reviewed [3].

Nevertheless, in the law enforcement content, in Europe (and beyond), the elements set out in the Budapest Convention on Cybercrime [4] provides a guiding framework on cybercrime, and many countries use this framework to classify cybercrime within their national reporting systems. Chapter II of the convention sets out each of the areas parties to the convention are expected to action. These are classified in the following way,

- Offences against the confidentiality, integrity and availability of computer data and systems
  - Illegal access
  - Illegal interception
  - Data interference
  - System interference
  - Misuse of devices
- Computer-related offences
  - Computer-related forgery
  - Computer-related fraud
- Content-related offences
  - Offences related to child pornography [sic][1]
- Offences-related to infringements of copyright and related rights

We can see an example of the instantiation of this taxonomy in the one used by the UK's Crown Prosecution Service (CPS) [5]. While still using the cyber-enabled and cyber-dependent distinction, the taxonomy effectively delineates between different crime types that can support investigators across

[1] *Here we are using the terminology as described in the Convention; however, Child Sexual Abuse Material (CSAM) is now the accepted terminology to more accurately reflect its status as an abhorrent crime with devastating impacts on the victims, rather than describing how the content is used.*

the investigative lifecycle and brings the language more up-to-date, although some of these aspects are included in the guidance notes on the convention [6].

Specifically, the CPS's taxonomy considers **cyber-dependent crimes** to include:

- **Illicit intrusions** into computer networks, such as hacking.
- **Disruption or downgrading of computer functionality** and network space, such as malware and (distributed) denial of service ((D)DOS) attacks.

This type of crime is present and within the scope of ENSEMBLE. Similarly, the descriptions of **cyber-enabled crime** include the following (in bold those specifically relate to ENSEMBLE),

- **Economic-related cybercrime**, including fraud and intellectual property crime, such as piracy, counterfeiting, and forgery.
- **Online marketplaces for illegal items**.
- **Malicious and offensive communications**, including communications sent via social media or other electronic means, cyberbullying/trolling or virtual mobbing.
- **Offences that specifically target individuals**, including cyber-enabled violence against women and girls ('VAWG'), such as disclosing private sexual images without consent, cyberstalking and harassment, and coercion and control.
- Child sexual offences and indecent images of children, including child sexual abuse, online grooming and prohibited and indecent images of children.
- Extreme pornography, obscene publications and prohibited images.

The first four bullet points of the above are also highly correlated with ENSEMBLE's target domains and use cases. Meanwhile, at the European level, Europol's EC3 (European Cybercrime Centre) focuses on three main types of cybercrime (for operations) – payment fraud, child sexual exploitation and cyber-dependent crimes.[2] On the other hand, the DG Home, via the EU Security Market Study [7], also developed a cybercrime classification. While helpful, it is worth noting that the genesis of this taxonomy is more oriented towards products and services than investigations. Nonetheless, the categories for cybercrime are,

- Attacks against information systems.
- Child sexual abuse.
- Digital forensics.
- Encryption and 5G.
- Non-cash payment fraud.
- Online identity theft.
- Dark net, including illegal markets and cryptocurrencies.

Within ENSMEBLE, these different definitions are useful for understanding the different facets and elements of cybercrime, the various aspects of the use cases, and in which areas of crime the technology developed can assist.

[2] European Cybercrime Centre - EC3. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

2.2 Prevalence of cybercrime in Europe

Compared to many other crime types, there is a lack of publicly available statistics at the European level on the prevalence of cybercrime at European and Member State levels, which is already known to be exacerbated by underreporting, by both individuals [8] and organisations [9]. Furthermore, while Europol, together with many LEAs, announce large takedowns or investigations that garner a lot of media attention for the efforts against cybercrime, the smaller-scale attacks against individuals or small businesses rarely reach the news headlines or are investigated at all, which leads to a multiplier effect on the underreporting [10].

The prevalence of cybercrime can be estimated from three main sources – crime reporting statistics, measurements of cyber-attacks and incidents, and victim surveys. These statistics may separately cover crimes against individuals and crimes against businesses (large corporations and small and medium-sized enterprises). Furthermore, cybercrimes can be targeted (i.e., an intention to attack a particular individual or organisation) or take a more indiscriminate scatter-gun approach (e.g., a widely distributed phishing email or malware distributed to all users who visit a particular website), which makes detecting prevalence even more difficult. A further key issue in underreporting is the perceived view that law enforcement is not well-equipped to respond to cybercrime-related offences [11], which reinforces the problem. Two current European projects – CYBBAR[3] and UnderServed[4] are both working to address some of these issues by improving the ease of reporting. One example of some indicative reporting of the prevalence of some types of cybercrime comes from Microsoft, who, in their launch of their recent European Security Program, highlight the countries in European most targeted by cyber-attacks (Figure 1 left) and the specific prevalence of the malware Lumma Stealer across Europe (Figure 1 right), where four out of ENSEMBLE's five end-users appear in the top-10 most targeted countries [12].

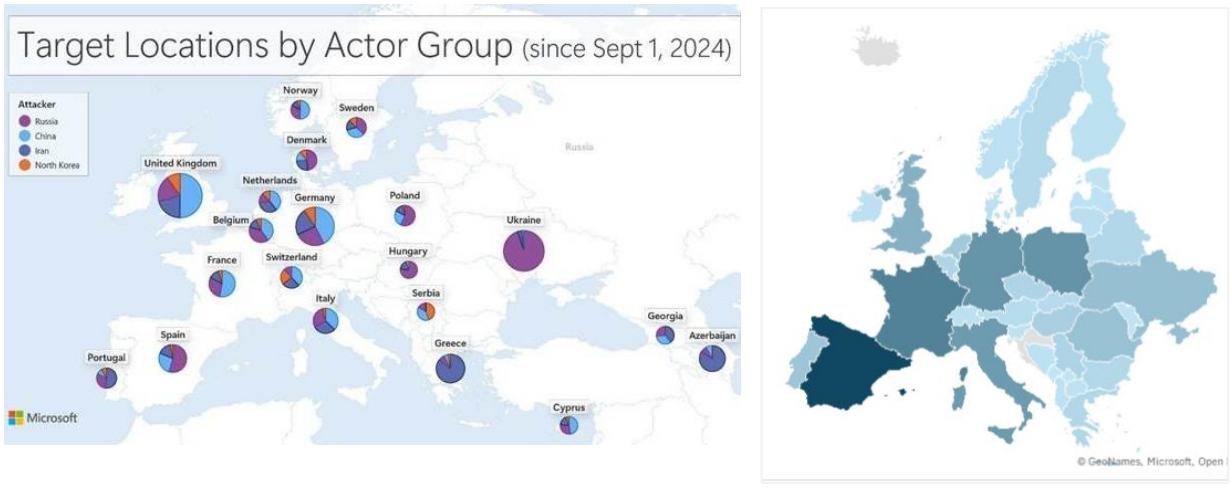

Figure 1: Examples of mapping the prevalence of different cybercrimes in Europe from Microsoft (left – countries most targeted by cyber-attacks, right – prevalence of the Lumma Stealer malware)

Since 2018, there have been calls for better reporting and analysis of the prevalence of cybercrime [13], including improving the quality and standardisation of victim surveys with a particular focus on a

[3] Cybercrime Victimisation Barometer (CYBBAR). Available online: https://cybbar.eu/

[4] UnderServed Cyber Threat Reporting Platform. (UnderServed) Available online: https://underserved-project.eu/

uniform categorisation of cyber offences to enable better cross-country comparisons, which differ drastically as seen later in the section. Currently, a recent Eurobarometer survey found that 28% of small and medium-sized businesses had experienced some form of cybercrime [14], while across industry 64% of leaders expect a cyber incident in the following year – which can have serious financial and reputational consequences for the organisation and for the individuals working there [15]. Furthermore, a separate Eurobarometer report on cybersecurity skills in organisations also highlighted gaps in skills and that in some countries (e.g., Romania) cybersecurity was seen as a low priority for an SME [16], which makes them particularly vulnerable to an attack.

Furthermore, the number of individuals who are victims of cybercrime continues to increase year-on-year. It is also worth noting that these crimes do not occur in isolation and have cascading effects across the crime ecosystem [17]; a cyber-attack on a large business, resulting in the exposure of personal data and passwords, can then lead to cybercrimes against individuals (such as fraud) or the widespread use of exposed email addresses on the dark web to launch phishing attacks (e.g., Group IB reports 6.4 billion records were leaked in 2024 [18]). Therefore, as with much of crime these days, there are links within and between different cybercrimes, involving various perpetrators, typologies, multiple victims, and occurring across jurisdictions, which will significantly impact how these crimes are investigated.

Within Europe, the most recent IOCTA report (2025) [19] emphasises the strong relationship between cybercrime and data, focusing specifically on the issues related to stolen or compromised data and how it is used to fuel other criminal activities. Particularly, they highlight how artificial intelligence (AI) and large language models (LLMs) are enabling much faster exploitation of data and how the same data is being used by multiple criminal organisations, often leading to the same victims being targeted more than once. Although working with breach data presents challenges for law enforcement ethics [20], the use of dark web monitoring and open-source intelligence (OSINT) tools, provide the opportunity to implement tools that support the early identification and tracking of online data breaches which in turn can support cybercrime efforts.

Although ENISA (European Union Agency for Cybersecurity) is aligned with cybersecurity rather than cybercrime, their latest cyber incident threat landscape [21] shows the scale of cyber-attacks which, in turn influences the rate of cybercrime. For example, the report highlights that the primary threats are ransomware, malware, social engineering, threats against data, denial of service, and information manipulation; all of which, except the latter, are featured or closely related to ENSEMBLE's use cases. In terms of law enforcement investigation into these crimes, the ENISA report highlights increased actions against ransomware groups and cybercriminals; however, these are typically part of much larger joint operations rather than in response to singular attacks.

At the Member State (MS) level, the amount of publicly available information on cybercrime varies across country. Below we briefly summarise the known current prevalence of cybercrime, and where available the rate of investigation by law enforcement in the different MSs contributing to ENSEMBLE.

Spain

Spain publishes regular cybercrime statistics and summarises them in a yearly cybercrime report. The latest report in 2023 showed that there had been an almost 100% increase in cybercrimes as a percentage of all crimes, rising from 9.9% in 2019 to 19.2% in 2023 [22], this encompasses **more than 470,000 reported incidents** and more than **350,000 corresponding victims**. The report notes that

crimes are classified as cybercrime according to the Convention on Cybercrime; but in addition, Spain classifies all crimes committed using technology as cybercrime.

Spain also provides valuable information about the resolution rate of cybercrime, i.e., how many crimes were reported/identified, how many had an effective resolution and how many arrests were made. In 2023, of all the cybercrime incidents identified **13.5% were resolved within the year** and over 17,000 arrests were made. This highlights a clear gap between the number of incidents and the effectiveness of resolution for the victims.

The same report also indicates which specific cybercrimes are most prevalent within Spain (in the reported data). In fact, offences related to **cyber fraud account for more than 90% of all cybercrimes, with most other crimes falling into categories such as threats and coercion, cyber forgery,** and unlawful access.

Additionally, Spain provides a wealth of statistics related to crime at both national and regional levels through its crime statistics portal [23].

Portugal

Portugal also makes available reporting and statistics on the state of cybercrime in the country [24]. Cybercrime in Portugal may encompass online scams, the illicit disclosure of personal data or photographs, and the dissemination of pornography. At least until 2023, Portugal does not separately record data for fraud that occurs online or offline, meaning that the scale of reports differs significantly from those described for Spain above and are not immediately comparable. Nevertheless, **Portugal is still seeing a significant increase in the cybercrimes recorded** (up from 193 in 2019 to almost 3,000 in 2023, and almost 4,000 in 2024) [25]. In general, the statistics show that on average 20-25% of reports of cybercrime received are then forwarded onto an investigation. However, this was significantly less in 2024, as many reports related to attempted fraud, but no fraudulent activity actually took place, and these were not forwarded for investigation.

The latest cybercrime report from Portugal also notes the recent increase in campaigns that represent the mass targeting of many individuals/organisations in the hope that some will fall victim to the scam, while fraud-related activity such as fake job adverts or contacts from police were present alongside more traditional cybercrime offences such as phishing attacks and the theft of account credentials. 'Newer' types of cybercrime seen in Portugal also include the growth of cryptocurrency investment scams and so-called 'hello mum/hello dad' scams which occur through SMS or online messaging platforms such as WhatsApp or Signal.

Romania

In Romania, one of the avenues for examining cybercrime prevalence is through the reports of DIICOT (Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism [English: Directorate for the Investigation of Organised Crime and Terrorism]. It is responsible for all organised crime, including the investigation of cybercrime, focusing only on the most severe forms of crime [26]. DIICOT reports annually on investigative statistics, including the number of overall cases and those closed [27]. **Since 2018, there has been a steady increase in cases** [28]**,** with just under 7,000 reported in 2024 in the area of cybercrime. Similar to other countries, the number of **cases closed each year accounts for approximately 25% of the total number of cases**. The report (p.35) indicates that the number of

outstanding cases has increased since 2023. DIICOT also provide some statistics related to how cases have been resolved, with around 14% through indictment or plea agreements, 21% by going to trial.

In terms of trends in cybercrime activity, Romania has seen an increase in SIM swapping activity (a form of identity theft) and a large number of phishing attacks targeting banking institutions directly in the country. Stolen mobile phones have also been used to falsely set up new banking accounts through the victims' devices. At the same time, an increase in the spread of child sexual exploitation material (CSAM) has also been observed. Similar to Portugal, fraudulent activity related to cryptocurrencies and the transfer of funds out of crypto wallets, as well as ransomware attacks, business email compromise (BEC), and CEO fraud, have also been reported. Relevant to ENSEMBLE, the cloning of websites to create fake pages, especially those related to banking and the financial sector, was also observed.

Moldolva

Moldova is currently in the process of improving its statistical capacity in the crime and justice sector,[29] thus there is less publicly available information than some other countries. Nonetheless, work done by Moldova in 2022, in collaboration with UN provides an initial baseline to work from. Due to the current geopolitical climate, Moldova is a significant target of cyber threats and attacks, with many of these targeted at the government, public and critical infrastructure sectors.[30] Nevertheless, Moldova faces an array of cybercrimes similar to those in other European countries – including various forms of online fraud and ransomware, as well as serving as a hub for cryptocurrency mining [31].

France

In 2024, France published its first annual report on cybercrime, looking at the activities and data from 2023 [32], while other agencies and organisations have also published supplementary reports. One piece of research has estimated that the **impact of cybercrime on France reached $93m in 2023 and could rise to over $400m by 2028** [33] highlighting the huge economic cost to society for such crimes, alongside the many other societal impacts.

As with all European countries, cybercrime is a rapidly growing threat in France. The most recent annual report showed that there were **more than 278,000 reported cases of cybercrime in 2023**, representing a 40% increase over the previous five years. This increase has led France to recognise cybercrime as a legitimate threat to national security [34]. It should be noted that France has a broad inclusion criterion for cybercrime, which also encompasses incidents such as online hate crimes. However, the main threats remain ransomware, online scams and fraud, and compromised personal data or information. Furthermore, despite the high numbers, they also warn that a significant number of cybercrimes remain unreported. Reporting cybercrime is made easier in France by the availability of three reporting platforms for the public: Perceval for reporting fraudulent use of bank cards, Pharos for reporting illegal content online and Theesee for reporting online scams. More than 550,000 reports were made via these platforms in 2023.

France divides its cybercrimes into four main categories, 59% of all crimes are classified as damage to property (e.g., scams and other activities leading to financial loss), 34.5% for crimes against people (e.g., harassment, threats, etc.), 6% were attacks on public institutions and 0.5% were crimes that violated specific legislation (e.g., the GDPR [35]).

ENSEMBLE has non-end-user partners located in other European countries that have shared data on cybercrime publicly, which are briefly summarised here. The **Netherlands'** most recent report on the

victims of online crime stated that 2.4 million people had been victims of online crime in the previous year. The majority of these incidents were related to online fraud (including phishing and identity theft), hacking (both devices and accounts), and online threats and harassment [36]. In general, all these trends have increased since the previous report in 2022. The report from the Netherlands also highlighted the societal impact of such crimes, such as leading to a reduction in trust and safety, as well as mental health impacts. Of those who responded, just under half said that they had reported the incident to a relevant agency, but only 18% directly to the police, again highlighting the gaps between incidents and official crime figures.

The most recent report (2023) from **Austria** [37] also highlights the **upward trend in cybercrime**, but a **decline in the clearance rate**, which has decreased from 35.8% in 2019 to 31.6% in 2023. In the case of online fraud, this is attributed to the increasing sophistication in concealing crimes (or perpetrators) and their associated professionalisation. Their reporting highlights specific trends in crime-as-a-service, blockchain and cryptocurrencies, pig butchering (a form of romance scam), hello mum/dad scams (also known as son-daughter trick) and similar payment and advertisement services, phishing, ransomware and ransomware DDoS, drug trafficking through the darknet, and CSAM.

The **UK** also reports several statistics related to cybercrime. The Crime Survey focuses on crimes classified under computer misuse, which, after experiencing significant decreases from 2019 to 2023, rose to its highest level in 2024, primarily due to an increase in hacking incidents. The CPS holds prosecution data, but there is no specific data on cybercrime. Currently ActionFraud [38] handles fraud and cybercrime-related reports and they have recently launched a cybercrime dashboard[39] with almost two-thirds of reports for cybercrime related to hacking of social media and email. Finally, and concerningly, in the UK, more than 50% of businesses and one-third of charities reported a cybersecurity breach or attack in the last year, with larger organisations reporting more prevalent attacks; however, in official statistics due to different definitions for cybercrime, these figures are reported to be 22% for businesses and 14% for charities for cybercrime [35].

In **Greece**, the Hellenic Police continue to lead efforts to combat cybercrime, as well as contributing to international operations, overall, around 13,000 reports of cybercrime were made, with around two-thirds coming through government reporting portal. Almost half of all reported cybercrimes related to fraudulent activities. In terms of investigation, almost 3,000 were forwarded to the prosecution directorate, while there were just over 500 arrests [40]. The report also highlights the awareness-raising efforts carried out by HP both through in-person efforts and also as online and VR games targeted at young people[5] – which are relevant for ENSEMBLE's future work.

In 2021, Grant Thornton made an extensive study of the cost of cybercrime in **Ireland**, where they had already seen a 50% increase in cybercrime with estimated costs to the economy be €9.6 billion [41], and this trend continued to increase in 2022 [42]. More recently, over a third of Irish households had experienced cybercrime in the previous year, with young people particularly vulnerable [43]. Similarly, recent analysis has shown **Italy** is one of the main countries targeted by cyber-attackers, with a higher than average percentage classed as 'high-impact' attacks [44]. While the Polizia Postale's report on cybercrime in 2024 found a continuing rise in financial cybercrime, especially through vishing/smishing

[5] CyberKid - https://www.cyberkid.gov.gr/

campaigns, as well as business email compromise (BEC). They also highlight the increasing issues they are facing with cryptocurrencies and the need for more highly skilled investigators.

Germany also reported a rise in cybercrime in 2024 [45], an interesting element from their report was that almost 60% of cybercrimes detected or reported came from outside of Germany (or an unknown location). In contrast to some other nations, Germany specifically saw an increase in distributed denial of service (DDoS) campaigns, especially by so-called Hacktivists; although ransomware remained the most significant threat overall. Economically, cybercrime is estimated to have caused more than €178 billion in damage [46], while concerns around how AI could accelerate cybercrime were also highlighted.

It is clear that most European countries are seeing an increase in cybercrime across Europe and that the main threat vectors are mostly aligned across the different jurisdictions. Similarly, where information is available, the volume of crime alongside the lack of reporting makes it difficult for cybercrime departments to effectively move forward to prosecution and see a resolution to the crime. Therefore, there are still significant opportunities to better support cybercrime units through a variety of approaches (e.g., tools, skills, training, resourcing, collaboration, etc.).

2.3 Actors involved in the cybercrime investigation process

Investigating cybercrime (or any crime) is not typically carried out by a singular expert. The nature and variety of crimes, alongside the highly technical domain, demand collaboration among personnel with a diverse range of skills and responsibilities. To support this, an extensive overview of the best practices for setting up a cybercrime investigation unit, covering team roles, responsibilities, training and internal and external collaboration has been prepared by CREST [47].

Complementing the above best practices of CREST, the Europol Training Competency Framework on Cybercrime (cTCF) documents the roles and requirements of all actors in the cybercrime investigation process, including those working in law enforcement, as well as those involved in the judicial process [48]. These roles are also matched with the skill sets needed to combat cybercrime effectively as described in Section 2.4.

The cTCF is extremely useful as a benchmark for understanding the cybercrime investigation landscape in Europe, as it maps out the actors and, by extension, the skill sets and activities that occur within an investigation. While the CREST guide focuses on the structural and procedural aspects of setting up a unit, the cTCF provides a detailed competency model that defines what each role must know and be able to do. The cTCF highlights 11 different roles within the cybercrime investigation process, noting that in some organisations, these roles may be merged and carried out by a single person or not required at all. Furthermore, the depth of expertise in core and sub-areas may vary across teams, depending on available resources, team size, or national context. A summary of each role is described below.

- **Heads of Cybercrime Unit** – primarily a coordination role focused on allocating staff and resources across a Unit; however, some practical hands-on experience is expected to enable effective evaluation of operational and strategic activities.
- **Team Leaders** – focus on coordinating and supervising cybercrime investigations within a specific area. They maintain a detailed overview of the team and should have some practical experience whilst liaising across the team and with the judiciary.

- **General Criminal Investigators** – focus on investigating other crime types but require a good understanding of internet-facilitated crime, electronic-evidence and how to handle digital material.
- **Cybercrime Analysts** – conduct information collection, analysis and produce intelligence, strategic analysis and research. They can also work operationally analysing information to spot patterns, trends and links across cases.
- **Cybercrime Investigators** – have additional capacity to seize electronic data, they may have an in-depth understanding of data extraction and interpretation, including from online sources. They may also conduct investigations, interviews and judicial processes, especially where it concerns digital evidence.
- **Specialised Cybercrime Experts** – typically have specific expertise on a particular cybercrime area (e.g., dark web, OSINT, cryptocurrencies, IoT, networks, etc.).
- **Digital Forensic Examiners** – focus on identifying, recovering, extracting, documenting and analysing digital evidence from different operating systems and devices using a variety of commercial and open-source tools. They have scripting and programming skills, understand forensics artifacts and may need to report and present their findings
- **Cyber-attack Response Experts** – liaise with CERTs and other IT/Information Security departments after a cyber-attack, they are responsible for recovering digital traces and evidence to support investigation and prosecution.
- **First Responders** – are LEA officers who are first on scene after an incident, they should have a basic understanding of cyber and forensics, they may need to secure fragile or volatile digital evidence and ensure the chain of custody from any digital devices on scene.
- **Trial and Appeal Judges** – generally they do not specialise in cybercrime but should have a good basic knowledge both cybercrime and e-evidence.
- **Prosecutors and Investigative Judges** – they may oversee criminal investigations and assess digital evidence, as well as authorising special means of investigation.

Based on the above descriptions, it is likely that ENSEMBLE will target **cybercrime investigators** and some **specialised cybercrime experts** (especially for dark web, OSINT, and cryptocurrencies) directly; however, in the wider scope the system would need strong relationships with digital forensic examiners, first responders, and cyber-attack response experts, particularly for receiving input or information. These roles are all integral to the handling, processing, and transfer of digital evidence during an investigation. Therefore, maintaining the chain of custody and evidential integrity alongside reports and outputs is crucial to serve the rest of the judicial system effectively.

2.4 Investigative skills necessary for cybercrime investigations

The same Cyber Training Competency Framework, namely the cTCF, also lists the main skill sets required for cybercrime investigation, and whilst this is not the only cyber-skills framework, it aligns Europe into a harmonised framework broadly applicable across all MS and cyber investigation actitvities. These skill sets are indicative of the activities that cybercrime investigation actors must undertake at various stages of the investigation process. These skill sets are divided into ten different areas.

- **General cybercrime knowledge** – knowledge of information related to cybercrime in general, with an understanding of cyber-enabled and cyber-dependent crime, cybercrime trends, threats, modus operandi, electronic evidence, and cybersecurity.

- **Specific cybercrime knowledge** – knowledge of specific cybercrime areas such as OSINT, dark web, blockchain/cryptocurrency, intrusion analysis and incident response, ethical hacking, threat intelligence and malware analysis.
- **Crime scene management and electronic evidence handling** – knowledge of best practices and standards for electronic evidence, including identification, seizure and working with volatile and non-volatile information. Additional non-technical crime scene management, interviewing and operational planning skills may be necessary.
- **Cybercrime investigative techniques** – encompass a broad skill set, including intelligence gathering techniques, data processing and interpretation, tracing suspects online and offline, conducting online undercover operations, questioning or interrogating cybercriminals, and risk management of an investigation.
- **Digital forensics (DF)** – covers several stages of investigation including identification, preservation, acquisition, validation, analysis, interpretation, documentation and presentation of electronic evidence. DF investigators may possess specialised forensic skills in areas such as live data analysis, operating systems, file systems, mobile devices, networks, IoT, cloud computing, and cryptography.
- **Network investigation and administration** – may include capturing and analysing network traffic data, identifying indicators of compromise to understand how networks function, and investigating events occurring within the network.
- **Programming and scripting** – skills in programming, scripting, and similar technologies can help with task automation, speeding up the analysis of large amounts of data and visualisation.
- **Reporting and preventing cybercrime investigation data** – covers documentation, chain of custody and investigative or technical reports. This may include the need to communicate complete information to different audiences.
- **Analysis and visualisation** – this involves using qualitative and quantitative data analysis techniques to identify patterns, trends, and actionable insights from cybercrime data. This can be for tactical, operational or strategic purposes; however, it is less focused on individual investigations, rather on combining information from multiple investigations and sources.
- **Cybercrime legislation** – having a good awareness of the applicable law at national and European level relating to cybercrime and electronic evidence, privacy, data protection, cross-border evidence exchanges and procedures for dealing with requests to and from non-EU countries.

While the above highlights the important skills for cybercrime investigation actors, a common outcome of any analysis of their needs is the requirement for better access to training, especially in the hands-on elements of an investigation. Training on cybercrime at the European level is supported by CEPOL (the European Union Agency for Law Enforcement Training),[6] ECTEG (the European Cybercrime Training and Education Group)[7] alongside many other specific providers. The UNODC (United Nations Office on Drugs and Crime) also provides a global programme on cybercrime training [49]. In CEPOL's most recent operational training needs analysis (OTNA) [50], it highlights that many investigators only classify their competency as being between basic and intermediate, which leaves a significant opportunity for enhancing training. The same OTNA also break down the training needs by cybercrime role type, emphasising that for cybercrime investigators, enhanced training is needed across almost all

[6] https://www.cepol.europa.eu/

[7] https://www.ecteg.eu/

areas, although it is not considered urgent, but should be addressed in the next couple of years. It is also noteworthy that analysts and investigative judges both emphasised the need for improved training in reporting and presenting information. Training for those working in the judicial system is offered at the European level through the Council of Europe [51], and the European Judicial Training Network (EJTN).[8]

The proposed use cases and tools developed within ENSEMBLE address many of these areas, including the need for general and specific cybercrime knowledge, as demonstrated through the use cases where common steps are applied across all investigative pathways, complemented by specific knowledge required in areas such as cryptocurrencies, malware analysis, and OSINT. A good knowledge of digital forensics, networking and analysis and visualisation align with the actions supported by proposed ENSEMBLE toolkit and are beneficial across each investigation. Furthermore, with specific training being created in the project for support in using the system and to support cryptocurrency investigations (building on CRYPTOPOL), there are significant opportunities for ENSEMBLE to also contribute to the upskilling of cybercrime investigation actors across Europe. In the next section we consider in more detail the specifics of the cybercrime investigation process, and the associated investigation techniques.

[8] European Judicial Training Network - https://ejtn.eu/

3 Cybercrime investigation process

There is no single way to investigate a crime; the individual activities are governed by the time of the crime being investigated, the information available, human and technical resources, and many other factors. However, in general, from the identification of a crime through to prosecution, there is a typical flow and process for the investigation to ensure the crime is investigated thoroughly and efficiently. Ultimately, the investigation aims to establish all the facts surrounding the crime, which enables the police to determine whether there is sufficient evidence to refer a person or persons for potential prosecution. As we have seen above, various roles are required to carry out the investigation process effectively. In this section, we provide a brief overview of the overall investigation process, the intelligence cycle, the requirements for evidence collection, and the roles of the judiciary and prosecutors, highlighting best practices and recommendations. Having reviewed the overall investigation process, we examine how these processes are currently customised to address cybercrime, incorporating current best practices and existing recommendations from research, as well as ongoing projects and recommendations from policing organisations themselves. ENSEMBLE, through its use cases, will consider several specific investigative avenues, including from the dark web to cryptocurrency investigation, ransomware/malware analysis, and the optimal presentation of information. The section concludes by examining best investigative practices from the information within the public domain in each of these areas.

3.1 Law enforcement investigations

The general process of criminal investigations is a well-established approach that can be applied across different crime types and jurisdictions. However, within that process, there can be specific investigative procedures that vary from country to country, between law enforcement agencies (LEAs) or departments depending on national laws, specific judicial processes and guidance, whilst the availability of resources can also be a factor. Nevertheless, the overall investigative process flow should be relatively consistent across jurisdictions. Typically, an investigation begins with an investigative trigger, which can be activated by a member of the public reporting a crime, by existing (proactive) monitoring processes, or other processes (the survey in Section 5 discusses the different investigative triggers for police authorities in ENSEMBLE in relation to cybercrime investigations). Typically, the first stage of an investigation focuses on responding to the initial trigger. The second phase involves the initial response and collection of evidence or intelligence to confirm the crime report. The third phase is typically the launch of the entire investigation. Depending on the severity and complexity of the crime, these phases can be relatively short or require extensive work.

The phases can generally be considered in accordance with the guidance from the College of Policing's Authorised Professional Practice (APP) [52]. The latter outlines standard investigative procedures in the UK. While it is not universally adopted in Europe, this guidance provides a useful reference model, and the stages are paraphrased below – focusing on the general steps rather than any UK-specific actions.

1. Identify the purpose and parameters of the investigation, recording any initial information to cover the who, what, where, when, and why of the crime/incident
2. Carry out checks relating to other on-going cases, resource allocation, recording, engagement with victims and witnesses and define first steps

3. Collect any initial evidence from the scene (physical or digital)
4. Follow initial investigative actions
5. Regularly evaluate the investigation progress
6. Follow further investigative lines
7. Consider victim and suspect support and management
8. Prepare files for prosecutor / judicial processes
9. Court and judicial processes

Not all of these phases are in scope for ENSEMBLE, where we are primarily focused on the intelligence and evidence discovery and analysis, and less so with the internal management procedures and engagement with suspects/victims, even though these are crucial elements of the investigation for ensuring a successful outcome.

Variations in this process between countries may include the need to obtain different authorisations at different stages to be able to continue to progress the investigation, as well as potentially different requirements around disclosure of evidence, retention of data or handling of devices. For instance, in some jurisdictions, investigative actions like surveillance, digital forensics, or seizure of devices require prior judicial authorisation.

Intelligence Cycle

While investigations typically follow a series of procedural phases, they are also supported by intelligence-driven practices. A widely used practice in this context is the intelligence cycle that is used for both defence and civil contexts, which defines an iterative process for collecting, analysing and evaluating intelligence. Naming conventions may vary, but typically it is composed of five stages: (1) planning, (2) collection, (3) processing and exploitation; (4) analysis and production; and (5) dissemination [53].

Activities in the intelligence cycle are closely aligned with those of ENSEMBLE, which has proposed numerous technologies for acquiring data, processing and analysing it, and then converting the information into evidence or a component of the judicial process. The intelligence cycle is typically referred to as a cycle, given that as one piece of intelligence is established, this can generate further needs for additional data or analysis. The collection of intelligence can come from numerous sources, including offline and online data, system exports, victim and witness statements, crime scene analysis, to name a few, and should be done in accordance with the principles of justifiability, proportionality and necessity. Furthermore, the processing, analysis and production processes can be enhanced and accelerated using semi-automated technologies that can rapidly and efficiently process large amounts of data. And, while many of these approaches may utilise AI, they also require a human-in-the-loop with appropriate knowledge to execute a clear judgement on the outputs of any technology [54], an approach that is mandated in the use of high-risk AI systems through the EU AI Act [55].

Additional considerations around the collection of intelligence might include the grading or assessment of the confidence level in the information – which can be a human assessment (e.g., based on the 3x5x2 model) [56] and/or as the output of an analytical model.

Evidence Collection

One of the challenges facing the increasingly digitised policing environment is the distinction and transition from intelligence to evidence, and how this can conform to the necessary standards. The

collection of information that aligns with evidential standards (maintaining the integrity and chain of custody) is essential to ensure it can be used in a court environment. In cybercrime, there can be increased complexity due to the higher likelihood of cross-border investigations. Therefore, a general harmonisation of standards across countries to ensure effective cross-border and joint investigations that all meet the required standards are particularly necessary, and have long been recognised as a challenge [57] across the entire criminal justice system [58]. At present, these rules are, in most cases, not standardised across countries, even within the European Union [59],[60].

The increase in digital information also presents numerous evidential challenges for law enforcement. Standards for digital evidence are defined in ISO 27037:2012, although this standard is primarily in the context of digital forensics, it also concerns network-based information [61]. This standard is also further supported by ISO 27042: 2015, which focuses on the analysis and interpretation of digital evidence [62].

Within ISO 27037, there are clear guidelines on how digital evidence should be handled, starting with compliance with the three principles: relevant, reliable, and sufficient. This is followed by the four key aspects specifically for handling digital evidence: auditable, repeatable, reproducible, and justifiable. Furthermore, it outlines the requirements for recording the chain of custody, including a unique identifier, access details (i.e., who, when, what, and why), and a record of changes. Systems that can automatically record this information with the necessary accuracy and detail are able to relieve investigators of this burden without compromising the investigation.

As the management of digital evidence moves forward with modern technologies, the available standards also need to keep pace. The LOCARD project developed a draft standard for the use of blockchain technology to support the chain of custody via smart contracts [63]. The standard covers initial data collection on-scene by first responders and follows through different acquisition and analysis phases, whilst also incorporating approaches to transfer of the chain of custody within and between organisations.

Standard Operating Procedures and Standards

Standard Operating Procedures SOPs) for police, investigative, or otherwise are typically prepared on a by-force basis, rather than at the national or European level. An example of a force publishing their SOPs extensively are Police Scotland [64] (e.g., their crime investigation SOP [65]). However, SOPs are not necessarily used extensively in investigative processes like those required for cybercrime. Instead, as discussed in the section above, the use of standards for digital evidence management is more common. Another relevant standard in this area is ISO 27043 [66] on Incident investigation principles and processes which aims at supporting the standardisation of the investigation process in relation to digital evidence covering all phases from readiness, initialisation, acquisition, and investigation alongside what they refer to a concurrent process – which includes management and administrative activity.

Some standardised processes have also been developed, which are more focused towards the cybercrime area whilst being aligned to ISO 27043. For example, a proposed ransomware investigation framework by Clancy [67] shows how the standard could be applied beyond its initial scope. Other standardised procedures at the European level focus less on specific practices but include areas such as police ethics [68] and the many guides produced by the Council of Europe's Octopus Community, which are primarily restricted to a law enforcement audience [69], as well as containing information

for prosecutors. Another example of a relevant standard is the ISO 27050 collection on e-discovery, which describes the procedures and processes for acquiring and handling electronic information whilst maintaining its auditability [70].

Role of the judiciary and prosecutors

The judiciary and prosecutors play a crucial role in getting investigations to court and ultimately for prosecuting offenders. However, even between European countries, the exact role of the judiciary and prosecutors can vary across countries. The Consultative Council of European Prosecutors (CCPE) even states, *"The role of prosecutors in criminal investigations varies from one system to another. In some countries, prosecutors can conduct investigation. In other countries, either the police can conduct investigations under the authority and/or supervision of prosecutors, or the police or other investigative bodies can act independently."[71]* Therefore, the Opinion from the CCPE sought to recommend the role for prosecutors in criminal investigations, in cases where prosecutors provide oversight of investigations their role may include providing instructions, advice, direction or guidelines to ensure compliance with criminal law and rights of the ECHR and ensuring that the evidence obtained, strategy, tools for evidence collection align with the needs for an effective prosecution, amongst other things. A separate workstream within the project is to interview investigators and judicial actors about their role, experiences and best practices in cybercrime investigations, the participation of at least one member of the judiciary/prosecutors will be prioritised to ensure their role is considered in greater detail.

3.2 Cybercrime investigation process

Cybercrime investigations can deviate from the traditional model of investigation, as described above, where a victim is identified, an offender (or offenders) is (or are) searched for through investigation, and evidence is obtained through both covert and overt investigative methods.[72] More than any other crime, cybercrimes can be investigated by a range of actors including private and public organisations' cybersecurity teams, by law enforcement agencies, regulators, or financial institutions. Each of these may follow a different investigative process – as they have different goals.[73] Furthermore, compared to some traditional crimes, cybercrimes often involve a significant distance between victims and offenders – often across borders and multiple jurisdictions, and many do not have a traditional crime scene. This all adds up to what can be an atypical investigative approach (in the case of investigative techniques and tools, investigative policy and strategy, legislation, and best practices), which leads to a lack of consistency across investigations, which can be a barrier for effective cybercrime investigations[72] and is a deliberate tactic of many cybercriminal to help evade detection or successful prosecution.

More than 20 years ago, Ciardhuáin [74] also recognised the need to adapt the traditional models of investigation that follow an identification, preservation/collection, classification/analysis, and reconstruction approach. Others have also attempted to update this investigation mode, e.g., Hunton [75], who also considered the stages of cybercrime investigation model from both technical and non-technical perspective and all actors involved, finding that a lack of resources, knowledge and training in cybercrime investigation was and still is hampering progress and efficiency in investigations. The view is corroborated by Gruber et al. [76] who highlight that LEAs are inefficient in fighting cybercrime, and while research proposes many theoretical models for enhancing investigations, these are not

necessarily easily translated into the real-world, may focus only on a small portion of the investigation or are not operationalised.

Additionally, the non-linearity and temporal variability of cybercrime investigations add further considerations. A useful, but US-centric, overview of the law enforcement cybercrime investigation process is provided by Bandler and Merzon [77] which covers many of the necessary considerations from data sources through to planning, investigation, alignment with regulations and collaboration with the private sector. While the categorisation of cybercrime investigation activities from the National Initiative for Cybersecurity Careers and Studies (NICCS) also provides a complementary overview of all possible tasks, knowledge and skills, similar to the cTCF.

At the international level, the UN Office on Drugs and Crime (UNODC) also maintain a public teaching series focused on different areas of crime, including a specific module on cybercrime investigation [78]. It shares information on all aspects of cybercrime, from introducing the topic to legal aspects, digital forensics, cybercrime investigations, as well as strategic and international cooperation aspects.[79] While the course is primarily aimed at those in tertiary education, in the cybercrime investigation section, it highlights several important considerations and best practices, for example, the potential for multiple police departments to collaborate in a single investigation, a lack of harmonisation in international laws and standards and the ability to collect data/evidence in a timely fashion. Meanwhile, on the technical side, investigators often face challenges related to proprietary systems and a lack of access to suitable technology. The course also reiterates the differences in cybercrime investigation processes across countries and the challenges this causes for international cooperation.

Similarly, the Interpol Cyber Strategy guide [80], while naturally focusing on more strategic aspects, also highlights some of the key areas to be aware of during investigations, such as underreporting (which affects LEAs' ability to make links between crimes) and the complexity surrounding cross-jurisdiction investigations. The World Bank also developed a guide for combating cybercrime, including best practices for investigations, but it appears unchanged since 2016 [81]. Nevertheless, many of the issues discussed regarding the basics of cybercrime investigation, legal frameworks, and investigator safeguards remain applicable today.

At the European level, the Council of Europe [82] has published SOPs for the collection, analysis and presentation of electronic evidence, and while aimed the 'CyberSouth', most are applicable more broadly, with extensive input from Romanian Police and contributions from Germany and the UK. The guidelines cover both technical and tactical guidance, although they should be checked for compliance with national laws.

In a similar vein, the OSCE has also published guidelines on cybercrime investigation [83], it discusses the different types of digital traces that could be considered as digital evidence on devices (from communications data, to logs, to cloud storage), information held by service providers/companies, such as basic subscriber information (BSI), and the principles surrounding preserving such evidence to maintain the integrity of any data. It also highlights the processes for ensuring the admissibility of electronic evidence (e.g., authenticity and veracity, use of fair and proportionate evidence gathering practices). It also underlines the importance of giving due consideration to how electronic evidence may be presented in court, noting that visual media are often more effective. Several potential types and sources of e-evidence are discussed, along with some methods for obtaining such data. The use of open-source intelligence (OSINT) is proposed whilst cautioning that the use of OSINT should be in line

with Article 8 (right to privacy) of the ECHR and that collection of such information should be necessary, proportionate and in accordance with the law. The guide also discusses cybercrimes directly, but only to provide an overview of the different types, rather than in support of an investigation.

A recent study into the investigation of money mules in the Netherlands [84], drew attention to the different approaches to investigation – the bottom up approach – investigating the money mules themselves – where approaches to improving the investigation could include better use of social media/OSINT and mobile device-related data; while the top-down approach focuses on the perpetrators in the layers above the mule and makes use of information such as IP addresses, cryptocurrency wallets, OSINT, and financial information. However, an emerging challenge in this case is that these investigations can become complex and voluminous quickly. The view of investigators is that the top-down approach tends to yield better intelligence, particularly for understanding the overall network. Such a consideration could be applied to wider cybercrime investigations.

Finally, from a research perspective, several academics have considered the current status of cybercrime investigations, initially starting with the models and approaches from Hunton [85], and often concurring with similar research noting issues related to underreporting and variations in the consistency of reporting, lack of knowledge and skills of some investigators (especially first responders), as well as the challenges posed by the area itself including cross-border aspects and the anonymity of perpetrators [86]. When academics have spoken to specialist investigators about the challenges they face they also still raise concerns about knowledge, skills and access to appropriate software, consistency of definitions, underreporting and under-recording, legal issues and those related to international cooperation [87], while others have noted there is extensive disparity between the capabilities and capacity for investigation between organisations (from tools to training to finances) [88]. A useful research result has been the model from Gruber et al., although it is not directly transposable into ENSEMBLE, they do provide a useful framework for consider the different layers of cybercrime investigation at different levels of abstraction, similar to the strategic, tactical and operational levels of planning found in more typical law enforcement operations. They suggest viewing cybercrime as three different layers,

1. A general process model – an overall model for an investigation broken into stages
2. Phenomenon-specific knowledge – a customised process for cybercrime and specific types of cybercrime
3. Case-specific concretisation – how the process actually occurs in individual cases.

This provides a good model for ENSEMBLE, and this deliverable, where we consider best practices for the general process model and specific phenomena related to cybercrime. Sections 0 and 0 describe the use cases and user requirements, providing case-specific concretisations.

Overall, despite these different approaches, there still appears to be the need for better classification of cybercrime, improved access to training and update/alignment of legislation, and it is worth noting for future training and guidance that a clear investigation process for cybercrime should be established, especially for the European environment.

From the judicial perspective, in 2020, Eurojust published an overview of some of the challenges best practices they face during their investigations or support for investigations, which were drawn from real-life cases [89]. Typically, as they focus on judicial matters, many of the issues related to mutual legal assistance or the speed of setting up a joint investigation team. However, they also highlighted

concerns where parallel investigations were being conducted in different countries, highlighting the necessity for international cooperation. Technical challenges aren't limited only to investigations; the report also flagged issues around encryption, use of cryptocurrencies and especially mixers or tumblers, or lack of availability of electronic evidence in general. Furthermore, the rise in smaller cyber-attacks (such as ransomware) also brings issues due to the scale and impact of such attacks, especially in criminal proceedings. Another judicial-related issue stemming from this is that, especially in cases related to organised crime, the same suspects can be under investigation in multiple jurisdictions, which requires processes for deconfliction. Data challenges were also highlighted, again emphasising the need for technology to make investigations more efficient.

Some of the concerns raised in the report by Eurojust, have been addressed in the intervening years. For example, cross-border access to electronic evidence was also made easier through the e-evidence package [90] brought forward through recent European legislation. The package composed of both a regulation and a directive, provides for the following actions, among other things

- European Production Orders – allow for faster cross-border requests for e-evidence compared to European Investigation Orders or Mutual Legal Assistance Treaties (MLAT).
- European Preservation Orders – allow for cross-border requests to preserve information ahead of a future request for this information
- Development of a decentralised system for communication between authorities and service providers

Regarding best practices, the Eurojust report also highlights some that directly impact investigations, such as the early involvement of the judiciary, especially to ensure the admissibility of evidence. However, their best practices are generally focused on when and how to involve Eurojust, but many cybercrime investigators also highlight that it is not always feasible or practical to run joint investigations due to the financial and human resources required [91].

As mentioned in Section 2.2 above, not all reported cybercrimes result in a successful prosecution. An analysis of cybercrime investigative failures identified issues with reporting and reporting systems, as well as the exchange of information between different units or organisations, among others. Recommendations included the access and acquisition of specific tools, as well as organisational factors (e.g., training, legal instruments) [92],[93].

Finally, ENSEMBLE does not exist in a vacuum in the EU research and innovation ecosystem. The knowledge, experience and outcomes of other Horizon and Internal Security Fund (ISF) projects have already contributed immensely to understanding best practices in different areas of cybercrime investigation – leveraging the experience of a wide range of end users. And, while some of these results are rightfully also restricted, we aim to capitalise on them where possible – especially for specific areas of good practices in cybercrime investigation. For example, CYCLOPES is focused on building a law enforcement practitioners' network[9] and regularly publishes updates on gaps, needs and challenges for cybercrime investigations across an array of topics and informed directly by practitioners which are explicitly referenced where relevant throughout this document. While others, such as LOCARD (on

[9] CYCLOPES – Cybercrime - Law enforcement practitioners network -https://www.cyclopes-project.eu/

lawful evidence collection) [10],INSPECTr (on intelligence analysis), INSPECTr (on intelligence analysis)[11] and Titanium (on financial and cryptocurrency transactions) [12] have their results interwoven throughout this report. Running concurrently with ENSEMBLE, are GANNDALF (cybercrime inter-agency information sharing)[13] and (crime-as-a-service)[14] who ENSEMBLE plans close collaboration and whose results will be incorporated into version two of this report.

3.3 Cybercrime investigation methodologies

In this section, we review different investigation methods for the crime types aligned to ENSEMBLE's primary use cases: ransomware and data theft – both from cyber fraud and unauthorised access and the best practices around the individual components of an investigation within cybercrime (e.g., OSINT, dark web monitoring, cyber threat intelligence, cryptocurrency investigation). Given the scope of the topic, these discussions are not intended to be exhaustive but focus on the key areas related to ENSEMBLE.

3.3.1 Ransomware

'Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom.'[15]

Ransomware (sometimes referred to as crypto-ransomware) attacks affect individuals, public and private organisations, large and small. The impact on the individual or organisation can be devastating, personally and professionally. Most commonly, ransomware encrypts the files and folders on a system and demands a ransom payment to unlock the files. Generally, individuals and organisations are advised not to pay the ransom as there is no guarantee that payment will lead to decryption or that the user will not be targeted again. Other types of ransomware include those that lock the computer screen, impact the computer booting process, encrypt web servers or target Android devices. [16] Initiatives such as NoMoreRansom provide mechanisms to identify the type of ransomware and decryption tools to assist users in accessing their files without submitting the ransom. Meanwhile, projects such as ransomware.live[17] provide detailed information about ransomware victims, groups, negotiations, notes, TTPs Techniques, Tactics and Procedures (TTPs), and Indicators of Compromise (IoCs) that can help support investigations.

[10] LOCARD - Lawful evidence collecting and continuity platform development - https://doi.org/10.3030/832735

[11] INSPECTr - Intelligence Network and Secure Platform for Evidence Correlation and Transfer - https://doi.org/10.3030/833276

[12] TITANIUM - Tools for the Investigation of Transactions in Underground Markets - https://doi.org/10.3030/740558

[13] GANNDALF - A Ground-breAking collaboratioN framework realizing the next era of cybercrime Detection And muLti-stakeholder investigation For LEAs, judicial ecosystems, and citizens. - https://doi.org/10.3030/101167951

[14] SafeHorizon - Innovations in Detecting and Disrupting Crime-as-a-Service Operations - https://doi.org/10.3030/101168562

[15] https://www.nomoreransom.org/en/index.html

[16] https://www.nomoreransom.org/en/ransomware-qa.html

[17] https://www.ransomware.live/

Recent research has charted the progress of ransomware, focusing on its evolution[94] and detection methods[95] including how and where it is typically detected and current mechanisms of defence (machine learning and non-machine learning based). However, for police authorities, the areas of interest are more likely to be related to the delivery mechanism, any engagement with ransomware-as-a-service (RaaS) models, and any features that can help to identify the perpetrators. In 2023, some of the main mechanisms used to deliver ransomware included phishing emails (often combined with social engineering), malicious advertising (aka malvertising), fileless attacks, use of various remote access methods, drive-by downloads, pirated software, network propagation – especially those that allow for lateral movement across the network, and RaaS approaches [96][97]. These are then combined with various attack vectors, such as email attachments, malicious URLs, exploitation of stolen credentials, or zero-day vulnerabilities. The NCSC [98] also created a clear graphic highlighting the main stages of a ransomware attack (Figure 2), while in a similar vein a crime script analysis by Matthijsse et al.[99] analyses in depth the eight stages of a ransomware attack from acquisition of the ransomware through to the cashing out process.

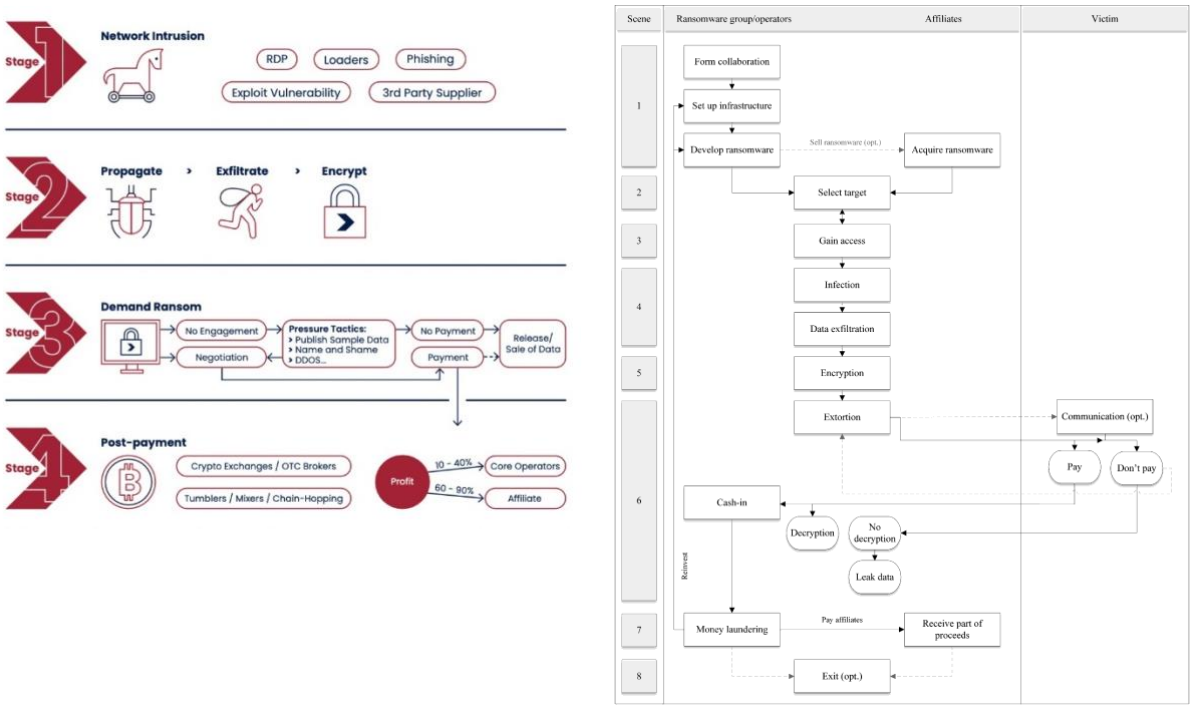

Figure 2: Ransomware Threat Methodology from the NSCS (left) and crime script analysis of a ransomware attack (right)

Crime script analysis can help to better understand the anatomy of a crime, by highlighting the attacker's steps, but it is a process that also provides a clear indication of areas that any future investigation can target. The paper also highlights important elements, including collaboration between attackers on underground forums and the outsourcing of attack process components, such as the use of initial access brokers (IABs) to facilitate system access. Another challenge of ransomware also links to the diverse opportunities for different responses and potential need for legal and policy reform to effectively combat its spread [100].

Ransomware investigation processes

While not all cybercrimes are always reported to law enforcement, it appears that reporting rates for ransomware to law enforcement (or an officially designated body) are generally high, although not all of those reports lead to specific investigative assistance [101]. When reported, given the multiple stages, potential data sources, and possibility of the involvement of various bad actors, the investigation process for police authorities and digital forensic investigators will likely need encompass multiple stages and activities. Furthermore, prior to the police investigation, if the attack has affected a company or large organisation, their internal cybersecurity team may have conducted a preliminary investigation. This may include verifying the original attack, documenting initial indicators of compromise, checking infected endpoints, and acquiring relevant data, such as network traffic [102].

As we can see in the generalised attack flow in Figure 2, there are several possible steps to an attack which need to form part of the investigation. Each of these stages gives law enforcement the opportunity to investigate different parts of the attack and search for relevant intelligence/evidence to assist in the investigation. In Table 3 below, we utilise the depictions of the different attack stages as described in Figure 2, and then the possible investigative actions a cybercrime investigator could take to further the investigation.

Table 3: Overview of attack elements and potential areas of investigation

Attack Element	Possible Investigative Actions
Ransomware Infrastructure	Analyse ransomware / malware type Identify Ransomware Group Identify RaaS seller / purchaser
Target Identification	Utilise open-source intelligence from surface and dark web (e.g., data leaks)
Access	Identify entry point & IoCs Check Initial Access Brokers
Infection and exfiltration	Analyse ransomware propagation Identify files / systems affected
Encryption	Check known decryption approaches
Extortion and Communication	Analyse ransomware note or chat / communication logs Identify crypto wallet and trace funds
Money Laundering	Trace funds, cross check mixers and off-chain transactions
Data Leak	Analyse breach sites
Collate information	Input information into MISP (Malware Information Sharing Platform) Visualise information through a dashboard and/or decision support system

Finally, considering the effectiveness of the ransomware investigation process, Meurs et al. [103] recently evaluated police authorities' interventions against ransomware attacks, focusing on five intervention strategies – arrest, takedowns, crypto-asset freezing, public decryptors and sanctions on ransomware groups, measuring how the ransomware group responds – ceasing operations, continuing operations or rebranding. Their research found that attacks with larger numbers of victims were more likely to lead to an investigation, while in just over half of the cases analysed, the intervention caused

a change in tactics for the ransomware group. They recommended that an increase in the number of interventions was more likely to disrupt activities compared to a single large takedown. However, a note of caution from a commentary on the UK situation highlights the likelihood that ransomware actors coming from Russia is high, which makes takedown and other disruptive actions difficult [104].

When considering how to move forward with ransomware investigations, many reviews suggest switching to a more proactive approach (such as the recent review by the UK's Joint Committee on National Security which suggests many agencies are ill-equipped to tackle the ransomware problem, regardless of whether those targets are individuals and small businesses, industry, or critical national infrastructure) [105]. Similarly, other research also suggests that more proactive approaches may be beneficial across the cybercrime spectrum [106] including what they term 'influence policing', which provides motivation for future awareness raising campaigns that can better support early intervention.

3.3.2 Cyber fraud, unauthorised access and data theft

The second core focus for ENSEMBLE relates to attackers somehow gaining access to data, information, files or similar from individuals or organisations and exploiting this information for further gain. Cybercriminals can deploy many different types of attack to gain access to information – this can include compromising or creating fraudulent online systems or forms leading to the interception of data or personal information (including usernames, emails, passwords and such like) through to more sophisticated attacks such a compromising social media and messaging platforms using deep fakes or other social engineering approaches. The information acquired can then be used to launch additional attacks or sold for profit. Alternatively, systems can be compromised through phishing or social engineering attacks, leading to the deployment of malware that can quickly exfiltrate significant amounts of data, often before the victim realises they have even been compromised. This type of attack can be further exacerbated by the attackers attempting to extort those affected by requesting payment to avoid the further exposure of information, which can lead to significant reputation and organisational damage or personal distress.

These types of attacks can be more complex to investigate than those associated with ransomware, simply because they can encompass many crimes in one, each of which causes cascading effects on the victim(s). Furthermore, there is much less in the public domain about how law enforcement executes their investigations for watering hole attacks or those that have utilised compromised forms or even been a victim of an online scam for a fake service, often because many people only report these attacks to their bank or other service rather than the police.

To investigate the various forms of online scams and fraud, law enforcement usually needs to identify and analyse the entry point to the crime – i.e., analyse the underlying code, incoming and outgoing connections, web hosts and similar aspects of the compromised form, site, or scam page. As mentioned, there has been little direct research on the topic – with current research directions focused towards victim perceptions and victimology [107], analysis of the cybercriminals and the spaces they operate [108], and even the legality of law enforcement using a watering hole-like attack to attract cybercriminals [109].

The first steps for law enforcement in investigating compromised forms, websites, and similar fraudulent activities include conducting an analysis of the website, while also in many cases working closely with telecommunications providers to ensure the website is taken down to prevent further

victims [110]. They can then progress to analysing the website code, connections, and related domains, extracting relevant indicators and metadata to start to build the picture of the investigation.

Scams related to cryptocurrencies, including crypto-jacking, so-called pig butchering scams, fake crypto exchanges, amongst others, are on the rise within the cybercrime domain. Current research has considered how law enforcement could more effectively investigate such scams, including by analysing the tactics, techniques and procedures (TTPs) associated with them or by using machine learning-based detection methods [111]. Some of these results highlight the limited lifespan of such sites (approximately one year) and the similarities between them. Another potential obstacle for law enforcement was the (mis)use by the website of Cloudflare Turnsite, which obfuscates the real IP address and prevents geolocation of the server [112]. Another suggestion was to correlate information between reverse registrant lookups to identify groups of scam websites; however, in most cases the registrant is hidden.

In the first phases of such investigation may be instigated and carried out by a digital forensics investigator to get a better understanding of the technical methods employed, although as Ribaux and Souvignet [113] explain the increases in cybercrime require the whole organisation to adapt to effectively investigate such crimes. Furthermore, where there has been an intrusion into an organisation's system, they may have deployed their own cybersecurity team in the early part of the investigation to extract relevant IoCs, logs and other metadata.

In terms of the investigation of crimes related to unauthorised access, whether that is related to cyber fraud, scams or direct attacks on the network, there appears to be limited research how investigators directly go about investigating such crimes and the direct processed followed. Further elaboration of this process will be prioritised in the next version of this deliverable and also contribute to the task on the future of the cybercrime investigation process.

3.4 Cybercrime investigation techniques

To address all the facets of a cybercrime, investigators need to employ a range of techniques and tools to acquire, analyse, correlate, and visualise data in relation to the attack. Furthermore, these techniques also need to maintain the chain of custody, ensuring the integrity of the digital evidence, so that it can be used to further the investigation. In this section, we explore a range of approaches, techniques and technologies that investigators can employ to support and enhance their cyber investigations.

3.4.1 Dark web investigations

Cybercrime on the dark web

The dark web is synonymously related with cybercrime. Bad actors utilise its increased (although not complete) anonymity to chat, sell and exchange information, products and services. And, while not all offerings turn out to be legitimate, it is a common starting point for cybercrime investigations. Particularly related to ENSEMBLE, the dark web is a platform for acquiring ransomware and malware, provides access to RaaS (and CaaS) offerings and initial access brokers, and phishing kits. It also serves as a hub for leaking and selling, as well as purchasing and accessing, breached data, among many other activities. Investigators can, with the right techniques and tools, identify crucial intelligence and

evidence from the dark web including marketplaces selling ransomware and data, usernames, cryptocurrency addresses and wallets.

In terms of the dark web itself, typically organisations are referring to ToR[18] as the most widely used dark net, although others like I2P[19] and Hyphanet (previously Freenet)[20] also exist. Regardless, dark web sites can often be transient in nature, often being available for short periods of time, and offer hidden services that regularly switch addresses or disappear altogether. Furthermore, tracing the location or providers of specific services is even more difficult, meaning traditional mechanisms of accessing or requesting the preservation of data from online services are unlikely to apply to the dark web, although more could be done regarding collaboration with hosting providers or ISPs.

Additionally, it is interesting to note that several organisations and outlets are now describing Telegram as the 'new' dark web due to its privacy features, whilst being significantly more convenient to access than traditional dark web sites [114], but with many of the same challenges for law enforcement investigations.

Investigating the dark web

Two of the largest challenges for dark web investigation are the lack of structure, making it difficult to search, and the ability for investigators to then effectively track, record and store the information collected from the dark web [115]. Of course, several commercial solutions exist to support investigators in their dark web investigations, but many are inaccessible due to cost and/or lack of training.

Furthermore, effective investigation of the dark web often needs to rely on two different elements of investigation: the use of continuous monitoring services for support in identifying and accessing historical data, particularly of services/sites that are no longer available or have changed over time; and the secondly more traditional dark web 'OSINT' where investigators directly interrogate and access various sites – which can be a manual or (semi-)automated process.

The needs of investigators related to the dark web are generally well documented but have not completely been addressed by developments over recent years. Typically, as with many facets of cybercrime training and legal requirements and restrictions have remained high priority needs [116]. Meanwhile, access to automated and standardised tools that enable effective and admissible evidence, development of practices that negate or counteract the increasing level of target hardening being used on the dark web, enhanced awareness of the utility of small pieces of evidence, e.g., pass phrases, PGPs, crypto addresses and wallets, and access to historic data are all considered as relevant technical needs to enhance dark web investigation.

Dark web monitoring

The ability to search and monitor dark web sites over time is essential for investigators who need to access both current and historical data where possible. This type of monitoring can be useful for both proactive and reactive investigations, although in ENSEMBLE we are more concerned with the latter. Unless LEAs develop and maintain a custom dark web database themselves, they are typically reliant

[18] https://www.torproject.org/

[19] https://geti2p.net/en/

[20] https://www.hyphanet.org/index.html

on commercial suppliers to access such data (e.g., CFLW[21], WebIQ[22], Searchlight Cyber[23], etc.), especially as searching the dark web itself is difficult task. The use of such monitoring tools can support the identification of trends, links between sites and activities and support with access to historical data.

The investigation process can incorporate dark web monitoring and dark web monitoring tools support access to search, query and alerting features, as well as reducing the risk for investigators to have to access the dark web directly [117]. The use of dark web monitoring services also helps what would typically be a resource intensive and time-consuming task [118] and allow investigators to accelerate their investigation whilst being able to correlate with existing data

Dark web investigation

Reactive investigations typically contain a OSINT dark web component that needs the investigator to either directly access and extract information from the dark web using their knowledge and experience, or at least have command of tools that can support the extraction of this data directly; however, if this is obtained in large quantities, access to analytical tools for processing data, text, images and video in a structured manner are also necessary (see Section 3.4.9). According to existing research, dark web investigation typically has three main aims/strategies - investigation, assistance and prevention [119]. For each of these steps, investigators then apply working methods and goals (1) identifying suspects' ID and locations for investigations, (2) identifying victims for assistance, and (3) communication, disruption and confiscation of unlawful funds for prevention of future crime. This is akin to OSINT investigations but customised to the dark web environment. Many of the tools used for dark web monitoring can also be used to support or alongside specific investigative actions.

In its 2020 report, Interpol recommended that all law enforcement agencies have access to technologies that facilitate access to the dark web, particularly those investigating financial crimes [120], while similar sentiments have also been highlighted by the FBI [121] alongside support for deconfliction of investigations. Further recommendations also include increasing the awareness of cyber hygiene practices specifically in relation to the dark web to ensure that any intelligence is collected lawfully alongside minimising the risk to the investigator [122].

A key component of dark web investigation is that it further uncovers other indicators and data that can contribute to or help to progress the investigation. For example, sites or accounts may expose IP addresses or other technical indicators [123], while posts may expose emails, wallets and other identifying information – such as similar usernames used across sites [124]. These can then feed into OSINT practices and cross over onto the surface and deep web (see Section 3.4.2).

3.4.2 OSINT and internet-based information

Open-source intelligence (OSINT) plays a critical role in online and cyber investigations. Due to the ever-expanding digital landscape, almost all crimes have an OSINT component; therefore, in this section we focus on the benefits and applications of OSINT to cybercrime investigations and specifically in relation to the core use cases within ENSEMBLE. The OSINT landscape is littered with best practices

[21] CFLW (2025) Dark Web Monitor - https://cflw.com/dwm/

[22] Web-IQ (2025) DarkCloud - https://www.web-iq.com/solutions/darkcloud

[23] Searchlight Cyber (2025) Cerberus: Dark web investigation - https://slcyber.io/dark-web-security-products/cerberus/

from many perspectives – from amateur enthusiasts, investigative journalists, corporate solution providers and through to current and former police investigators, thus it is essential to focus, where possible, on techniques and approaches that are suitable for the law enforcement domain, including those that maintain and prioritise the chain of custody and evidential integrity.

Relationship between OSINT and cybercrime

In the areas that ENSEMBLE focuses on, OSINT might be used to verify information in a ransom note, cross-check information exposed through a data leak, complement information related to a cryptocurrency transaction, link a username, email or phone number found on a dark web advert, or support cyber threat intelligence activities. Furthermore, while not strictly always OSINT, chats, channels, and communities on online messaging apps such as Telegram, WhatsApp and Signal are also playing a greater role in investigations. Rahman has carried out a useful overview of potential online sources of information relevant to cybercrime [125]. Other OSINT tools may include those for exploring domain names, IP addresses and other types of publicly available information. Information from OSINT can also make a valuable contribution to cyber threat intelligence (see Section 3.4.7), including being imported into MISP [126].

Now forming part of OSINT investigations can include breach or leaked data – this can be particularly useful to law enforcement when trying to resolve identities or find further information. However, there is also an ethical conflict relating to law enforcement potentially benefitting from exactly the kind of data breaches they are trying to prevent [127].

A further challenge for the effective use of OSINT is continuously and rapidly evolving online landscape that can render known techniques useless with the change of an API or format of a page or the deactivation/deletion of a social media profile, not to mention the different online services that can change in popularity with different demographics, countries and the task at hand. Therefore, time can be an important factor in the effective use of OSINT.

Investigations using OSINT and internet-based information

The OSCE's guidelines on cyber investigation provide an excellent overview for law enforcement of the different steps and applications of OSINT in cybercrime investigation [128]. Prior to any OSINT investigation, good operational security is essential, meaning the investigator may need to limit their online footprint and use appropriate software and devices that help to restrict or eliminate attribution. Taking care to record collected information effectively and in line with requirements for the chain of custody are also essential, this might include the use of covert online personas for a variety of social media services and logging the activities of each account. Furthermore, using approaches that assure the need for the acquisition of information is necessary and proportionate to the scale and type of investigation and limits the possibility of collateral intrusion.

Recently, the CYCLOPES project, analysed the main needs and challenges for OSINT investigators in the area of digital forensics and cybercrime, these included needs around support for aggregating data across different sources, as well as language and analytical tools, and the management of online alias for investigators (a challenge that has been tackled by the HEROES project[24]).

[24] HEROES - Novel Strategies to FigHt Child Sexual Exploitation and Human TRafficking Crimes and PrOtect thEir VictimS - https://heroes-fct.es/investigation-en#

The collection of OSINT for investigations can utilise both manual and automated collection techniques, depending on the specific goals of the investigation. Automated scraping and collection tools support investigators when larger amounts of information from sources such as marketplaces, forums, paste sites or even source code [129]. OSINT for cyber investigations also includes support for activities such as cross-checking information in public databases, including aspects such as checking domains, IP address, ports, subdomains, server configurations and others[130] Furthermore, investigators also use OSINT to identify crypto wallets and addresses, while Gupta et al. [131] highlight how OSINT and digital forensics can go hand-in-hard to improve investigations, especially in making better use of data from cloud and device storage [132].

Additionally, the use of OSINT can also bring with it investigative risks, therefore it is recommended for investigators to employ good cyber hygiene practices during their investigations. This includes the use of VPNs, authentication measures, appropriate data handling procedures and managing the investigators online footprint, as well as working within organisational regulations, policies and requirements [133].

3.4.3 Networks and servers

When a cyberattack has compromised a network or computer infrastructure, there are numerous opportunities to extract valuable information and indicators of compromise related to the attack itself. For example, investigators may be able to locate relevant IP addresses or find those IPs from malware or ransomware that link back to the command and control (C2) servers. Local network analysis may be able to pinpoint incoming and outgoing network traffic (using tools such as Wireshark for packet capture).

Where the investigation centres around a larger organisation, their cybersecurity teams may be able to provide information from intrusion detection systems (IDS) and other network monitoring tools to assist the investigation. This is one area of cybercrime investigation that can be more collaborative or require law enforcement to work directly with the organisation that has been subject to the attack to receive relevant critical data.

Receiving, extracting and analysing information from networks and servers

During an investigation, the analysis and interpretation of this information may be assigned to a cybersecurity or digital forensics specialist, where they may be supported by CERTs (Computer Emergency Response Teams) or CSIRTs (Computer Security Incident Response Team). For the most part, ENSEMBLE is concerned with the offline analysis of network data, i.e., it has been obtained through another tool; however, investigators may face issues related to encryption (of the network traffic) and interpretation (such as from the move away from standardised ports, use of covert channels, and increased number of approaches for anonymity) [134], while where there is signification amounts of traffic – their ability to process data can be impeded.

Where law enforcement needs to directly investigate network and server infrastructure, this may fall more towards cybersecurity or digital forensics specialists; however, cybercrime investigators will need to be able to understand and contextualise the information acquired to link it to other aspects of the investigation – including CTI aspects as discussed below.

In terms of network forensics, in the reactive cybercrime investigation process, law enforcement is more likely to employ the *'stop, look, listen'* approach that captures network traffic data only after an

attack has happened (although data from more proactive monitoring may be available from larger organisations' security teams) [135]. Especially in this latter area, there is significant potential to employ AI-based techniques to more effectively identify attacks or compromises at an early stage.

A separate focus for investigators is the attribution process, and while this may combine information from other parts of the investigation, is also an approach in its own right. The use of TTPs (see Section 3.4.7 below) can help to support attribution by identifying where similar approaches have been used in other attacks -establishing a modus operandi [136].

3.4.4 Cryptocurrency investigations

Role of cryptocurrency in cybercrime

The cryptocurrency element is an ever-growing component of cybercrime; even four years ago, Europol was highlighting the extensive criminal use of cryptocurrencies [137]. Since then, the array of cryptocurrencies and privacy coins available has increased rapidly.

In the CYCLOPES' analysis of the gaps and needs of LEA practitioners in the area of cryptocurrencies [138] core challenges for police authorities were recognised as the fragmented legal framework, difficulty in acquiring tools due to cost, the need for automated tools for analysis – including user friendly reports, the need to also trace privacy coins such as Monero and tools to support tracing through mixers and tumblers. The report also flagged that additional support is need for prosecutors in this area. The majority of these needs still appear to be directly relevant to investigations today.

Investigating cryptocurrencies

The end-to-end process of just the cryptocurrency component in an investigation can encompass numerous steps. This starts with the identification of cryptocurrency transactions, addresses and wallets, which LEAs can then begin to trace. If cybercriminals are using chain-hopping approaches, mixers or laundering the money through different currencies, the investigation becomes more complicated within multiple pieces of information to keep track of [139]. Generally, most solutions for cryptocurrency investigation include visualisations of graphs and supporting graph analysis, while integration with OSINT solutions to link to off-chain information other financial services also be beneficial. Meanwhile, investigators often also require additional support for tagging and/or the inclusion of additional metadata to complement the transaction information.

Given the way cryptocurrencies have exploded in use and number over the last 5-10 years, there is an extensive number of articles, solution providers and guidebooks offering approaches to effectively investigate cryptocurrency information (e.g, on bitcoin tracing [140], money laundering [141], and broader overviews [142]) In TRM's 2023 survey of law enforcement [143], they highlighted the relative complexity of cryptocurrency investigations, especially when criminals are aiming to directly obscure their activity and employing chain hopping or crypto swapping techniques (and even more so when tools do not directly support the analysis of such activity), and cross-jurisdictional challenges. Lack of tools directly aligned to their investigative need was also highlighted as a significant challenge.

Tracing, of course, the availability of the blockchain or other public ledgers provides an advantage for police authorities during their investigation, as such records are somewhat more easily accessible than many other data sources, despite a wider belief in the public arena that cryptocurrencies can be somewhat anonymous [144].

Along with many other forms of cybercrime, legal challenges also arise during the investigation of cryptocurrencies; furthermore, as there is little regulation in this space, there is significant diversity in approaches across jurisdictions [145]. In particular, an advantage of better regulation would lead to improvements in attribution for police authorities during their investigations – although effective cybercriminals may mitigate against this through chain hopping and mixers.

A recent guide to best practices in cryptocurrency investigation produced by the Blockchain Intelligence Group provides a detailed step-by-step approach to role of cryptocurrency in different cybercrimes – such as money laundering, investment fraud, ransomware, phishing, dark web, and various other scams [146]. The guide introduces common terminology, types of crypto wallets and a number of different tools and how they can be applied during the investigation. Further explanations on how KYC (Know Your Customer) and AML (anti-money laundering) regulations can support access to additional data held in crypto exchanges as well as other legal routes. Their recommendations for best practices investigation focus primarily on evidence capture from hardware and software wallets, with limited direct investigation guidance, although they champion collaboration between LEAs and with financial institutions as well as the wider community. In terms of investigative advice, they also highlight best practices relating to when to stop tracing to enhance investigative efficiency.

A similar guide from the OSCE [147] recognises the challenges and issues faced by investigators in cryptocurrencies, such as incomplete data and misunderstandings around which data are needed. The OSCE, along with many other guides, also highlight the need for better training for LEAs in cryptocurrencies – something that ENSEMLBE will also tackle by building on the experience of Cryptopol [148]. The guide describes best practices for investigating different types of cryptocurrency transactions (FIAT to crypto, crypto to crypto, crypto to FIAT). They also list the different types of crucial information/evidence for investigators to collect, including from individuals, crypto wallets, and VASPs (virtual asset service providers), and the advantages, potential pitfalls and limitations of each piece of data. The guide then also supports the transition of moving from intelligence collection into evidence that can be used in court, including the type of information available, analysis undertaken, and the need for reports and effective presentation of evidence.

Securing and ensuring the evidential value of crypto-assets is one of the biggest challenges faced by investigators and tool providers alike, with concerns existing around the evidential value and the extent to which such information will be accepted at court, with suggestions of utilising attribution and tags to improve the tracking of the provenance of the data and analysis, or by using approaches that assure the reproducibility of the acquisition and analysis [149].

Other investigation challenges recognised during analysis include issues with the cost of commercial tools and the computing power required for open-source alternatives coupled with a lack of expertise alongside wider investigators [150]. Furthermore, communication flow around problematic wallets is often hindered. There is a call for better policy and procedure to be created around cryptocurrency investigation for LEAs, including how to handle, store, transfer and redact keys within systems.

It is also useful to consider best practices that complement cryptocurrency investigation also include leveraging more traditional finance data as well as looking into off-ramps [151] which can help with attribution or corroborating ownership or destinations of funds, as well as looking into patterns relating to the movement of funds. Meanwhile other

Interesting other propositions for investigations to utilise in order to enhance their cryptocurrency investigations include better integration of confidence values for different types of evidence and opportunities for combining them, making use of temporal and other patterns to support privacy coin and cross-chain analysis, and leveraging lapses in operational security for investigator benefit [152].

3.4.5 Requests to online service providers and third parties

Role of OSPs in cybercrime

An increasing amount of data related to cybercrime investigation is now stored in the cloud or is retained by online services – which may be social media services, virtual asset service providers (VASPs), hosting service providers (HSP) and cloud service providers (CSPs). The result of this is that many external organisations may hold data significant to an investigation. The challenge for LEAs is then getting access to this information, that may be basic subscriber information (BSI) [153] or more complete information. For entities established in the same jurisdiction, these requests may be relatively straightforward; however, for services in other jurisdictions, LEAs may need to rely on existing relationships, the mechanisms provided for in the e-evidence package, or the in the worst-case scenario – use of mutual legal assistance which can be prohibitively slow for a fast-moving investigation with a significant number of digital components. Furthermore, as privacy campaigners are highlighting to citizens the types of data law enforcement could potentially access [154], it could lead to such information being available for much shorter periods of time, making the European preservation orders even more

Incorporating OSPs and data into investigations

In terms of cybercrime, these requests can often initially begin with basic subscriber information, but as the investigation progresses, there may be a need for access to additional information if held by the organisation and relevant to the investigation. Within Europe, Europol provide information in collaboration with Eurojust through the SIRIUS project [155] about obtaining electronic data from other jurisdictions including best practices, forms and templates for making efficient requests. However, it is now recognised that a significant barrier facing LEAs is encryption – with current decryption tools consuming more resources and being less effective [156],[157]. The Council of Europe, in collaboration with the European Union, has also published guidelines of best practices for cooperation with internet service providers (ISPs) [158]. Other challenges also include tools for accessing such data, as well as obtaining credentials that may facilitate access; furthermore, the large amount of data obtained from these providers presents a challenge in itself [159].

For online service providers outside the jurisdiction of the LEA, the aforementioned e-evidence package provides for improved processes in making requests to third-party organisations. Finally, from a forward-looking perspective, the European Commission, through its High-level expert group on access to data for law enforcement, have published a 'Roadmap for lawful and effective access to data for law enforcement'[160] which includes further development of the Sirius project, including a unified catalogue of data that electronic communications providers provide – which could also support technology providers and subsequently investigations by enabling easy import of such data into intelligence systems.

3.4.6 Ransomware & malware analysis and other site analysis

Analysis of ransomware, malware and other code

When ransomware or malware is deployed onto a machine or system, there is also the opportunity for digital forensic investigators to analyse the underlying code and code structure to help identify clues about how the malware was propagated, uncover indicators of compromise and extract information about who may be behind the dissemination process.

Malware analysis is typically performed by digital forensics experts or those who specialise in such areas. Although access to such expertise may not always be possible, in some cases, law enforcement agencies may partner with the private sector to carry out such analysis [161]. However, this may not always be possible for all investigation teams. Alternatively, Investigators can obtain useful data through the analysis of ransomware or malware deployed in a cyber-attack. Historically, Europol made their malware analysis solution [162] available to LEAs although it is not clear how this has developed since 2015, but it is still referenced in recent programming document (e.g., 2023 – 2025) [163] and Europol also provide support to the NoMoreRansom project which supports the analysis of ransomware, to help provide tools for the decryption of any files.

Use of ransomware/malware analysis in investigations

The benefits of malware analysis in support of law enforcement have long been recognised as a vital component of an investigation for its ability to understand how the malware interacts with other online services, the type of information targeted by the malware and find commonalities with other malware from other investigations [164]. Information might include receiving commands that allow the investigator to identify a C2 site that instructs the malware, or connections related to the exfiltration of data. The Malware Analysis Framework provides an extensive overview of all aspects of malware analysis and the types of intelligence that it may be possible to extract, as well as guidance on information sharing [165].

Malware is often deployed and then discovered directly on a live digital device, and if it needs to be analysed directly, it would be necessary to utilise a digital forensics or cybersecurity expert who can carry out live forensics. On the other hand, post-incident, investigators may only be able to investigate the malware in a sandbox environment where nicknames, online resources, email addresses, or outbound connections can be extracted; alternatively, they may only receive hash values [166]. Malware analysis can incorporate multiple stages, including static and dynamic analysis of the code[167] although savvy cybercriminals will employ techniques to evade detection which make the analysis more complex and are more likely to require specialists to carry out [168]. Investigators can also make use of solutions such as the malware analysis tool evaluation framework to support the selection of relevant and available tools for the analysis [169].

3.4.7 Exploiting cyber threat intelligence

A perhaps underutilised resource in law enforcement investigations is the specific and strategic use of cyber threat intelligence (CTI) to support and enhance investigations, including identifying links and patterns across different attacks and incidents. Despite the presence of literature on its usefulness for law enforcement since 2013, its application remains underutilised [170]. CTI needs to be actionable for law enforcement, and although sharing initiatives such as Interpol's Project Gateway already exist, law enforcement needs to be not overwhelmed by the amount of information shared with them to utilise it effectively [171].

A recent study by the UnderServed project focused on the exchange of CTI between NGOs and law enforcement (although the results are also applicable in other areas such as for SMEs). This report

highlighted the challenges faced by NGOs in sharing good CTI data with law enforcement, which consequently means LEAs do not have the information required to act upon many cyber threats in a timely manner [172]. The project's outcomes have led to the creation of a more efficient reporting platform for NGOs and other organisations, which can help feed information to LEAs via the Malware Information Sharing Platform (MISP) (see below) [173]. These types of initiatives help to address the incoming streams of information, but alongside this, law enforcement must also make effective use of CTI when they receive it.

The most basic form of CTI are small pieces of data, known as IoCs, that suggest some form of malicious behaviour has occurred. These technical artifacts may be exported from systems or log files and include things like file hashes, IP addresses, and domains addresses, as well as more complex technical artifacts. IoCs are typically linked to a specific cybersecurity incident and help form the underlying evidence base. As CTI analysis gets more complex, investigators may make use of frameworks such as the Cyber Kill Chain [174] and MITRE ATT&CK [175] to help map out tactics (the behaviour of a threat actor), techniques (the execution of the behaviour) and the procedures (the specific tactics employed for the attack), collectively known as TTPs. The MITRE ATT&CK framework provides a common language for documenting and describing cyber-attacks, facilitating better information sharing and consistent terminology. The different elements of the framework are aligned to one of 14 different stages from reconnaissance to exfiltration. Efforts have also been made to customise it to the law enforcement investigative environment [176].

The benefit of using CTI in cybercrime investigations include the use of the ATT&CK matrix navigator to help to map out and understand the flow of the events after a cyber-attack[25] while law enforcement can also leverage platforms such as the Malware Information Sharing Platform (MISP) to collect and share CTI-related information at different levels, typically governed by the traffic light protocol (TLP) and the permissible actions protocol (PAP).

Use of CTI in cybercrime investigations

Typically, CTI is currently underused in investigations, due to a combination of lack of awareness and knowledge, limitations around information sharing, and lack of access to technical infrastructure, as well as lack of understanding of the potential benefits CTI can bring to an investigation. In fact, challenges in CTI sharing are not just an issue for law enforcement but for many organisations [177]; however, the introduction of more automated sharing mechanisms and improved identity and access management that allows finer control on the information shared is expected to enhance this process.

CTI can include information about recent and historical attacks around the world, which may provide useful intelligence; however, LEAs should use caution when utilising crowd-sourced CTI datasets or data feeds as many have not been independently checked for accuracy [178].

Capitalising on MISP in cybercrime investigations

The Malware Information Sharing Platform (MISP) is one popular environment for effective sharing of CTI within and between teams and organisations, the other being OpenCTI. The advantage of using a platform like MISP is its ability to correlate information such as IoCs and TTPs with open-source information, whilst also utilising structured knowledge in the form of shared taxonomies, naming

[25] https://mitre-attack.github.io/attack-navigator/

conventions and similar. MISP is structured so that each cyber-attack or threat is called an event, each event can have multiple objects which bring together groups of attributes related to the event. Attributes can be IoCs or other small pieces of information.

As the MISP interface becomes richer with information, investigators can use the platform to both interpret and act on information with MISP. By correctly utilising the CTI, investigators may be able to establish attribution, connect multiple indicators together and link them directly to their case, quickly assess the severity or urgency of the threat and help to establish the confidence or accuracy of the intelligence. The key features of MISP include correlating indicators (especially between events), constructing event timelines and graphs to demonstrate the flow of the attack and how different elements are linked together (this can be accelerated by importing logs and other information), applying taxonomies and tags to enrich the information in MISP further and structure it for effective case development, utilise wider taxonomies of information (known as galaxies) to introduce domain specific information, enrich the existing information with OSINT and correlate information across cases, and finally produce and export information as customised reports [179].

Recognising the potential value of MISP, the MISP-LEA site[26] provides LEA-specific information about the MISP platform specific to the LEA environment, LEA-specific training materials and access to collaborative resources. MISP currently promotes two user stories for the use of MISP in the law enforcement environment [180] as shown in the table below. These show the envisioned use cases for MISP within the law enforcement environment. MISP also provides APIs, thus allowing developers to build upon the information in MISP and customise it to their own needs and requirements. ENISA also recommends the use of MISP to support collaboration between CSIRTS and law enforcement [181].

Table 4: Example from MISP of potential use cases for law enforcement

As a law enforcement officer, I want to investigate digital crimes and threats so that I can apprehend criminals	As a law enforcement officer, I want to collect and verify evidence of digital crimes so that I can bootstrap my DFIR cases
• Access information sharing communities • Get indicators and actionable information from CSIRTs/CERTs networks or researchers • Exchange information with other officers via sharing communities • Exchange and store incident information on MISP, enabling the system to act as a forensic tool over time	• Collect indicators from shared events • Propose changes to existing analysis or reports • Enhance existing events with additional pieces of evidence using Extended Events • Exchange analysis and reports of digital forensic evidence • Correlate indicators corresponding to forensic pieces of evidence • Import Mactime timelines to describe forensic activities on an analysed file system • Describe forensic analysis cases using objects templates • Create, modify and visualise the timeline of events • Share analysis and reports of digital forensic evidence

[26] https://misp-lea.org/

	• Report sightings such as false-positive or true-positive (e.g. a partner/analyst has seen a similar indicator)

One of the biggest challenges for effective use of MISP is the user interface is not necessarily easy to use and has a relatively steep learning curve, which may put investigators off engaging with the tool in its current form, especially for visualisations [182], which is another challenge addressed by ENSEMBLE, both for MISP and wider intelligence analysis.

3.4.8 Visual intelligence and analytics

A common requirement from law enforcement across the cybercrime domain is the need for efficient and effective data analysis and visualisation features, alongside export and reporting capabilities that can effectively support investigators in extracting intelligence from available data and converting it into a format that also helps bridge the gap between investigation and the judicial process. Nevertheless, the visual intelligence and analytical capabilities provided or used by investigators should not simply be a more interesting way of presenting the data; they need to be functional and easy to use. They must provide investigators with the data they need accurately and quickly, allowing them to work with the system not against it. Cybercrime investigations can generate substantial data, making it essential to have searching, filtering, querying, combining, and analysis functions that provide value to the investigation.

Separately, during the transition from investigation to court, it is often necessary to export and report information gathered during the investigation in an easily understandable manner, which can be presented to the judge or prosecutor, and even the jury.

Visualisation and visual analytics in cybercrime investigations

Almost all the facets of a cybercrime investigation discussed in this chapter require or can be enhanced by some form of visual representation. Whether that be through tables, charts, graphs, or other visual representations, these elements must work cohesively with the data the investigator has access to. Cryptocurrency investigation is already a strong example here – with most cryptocurrency tracing tools providing overviews through node-link diagrams, while similar approaches are also available in MISP for CTI, and many OSINT-related tools utilise networks to show links between entities and activities (e.g., Maltego,[27] Linkurious,[28] Cambridge Intelligence,[29] etc.).

Many visualisations and visual intelligence systems currently developed focus on the cybersecurity monitoring aspect [183] rather than the reconstruction and reporting element which are either not prioritised or well publicised as available solutions. In this regard, VizSec has a long history of publishing cybersecurity-related visualisations for law enforcement and other cyber-investigation purposes, each visualising different types of cyber-related data.[30] Others take more ad-hoc approaches developing

[27] https://www.maltego.com/

[28] https://linkurious.com/

[29] https://cambridge-intelligence.com/

[30] https://vizsec.org/

their own systems or visualisation using standardised tools such as Power BI[31]. However, this puts the onus on the investigator(s) to continue to keep the tool up to date and is at risk from changes in personnel. In general, the research interest in visualising cyber-crime and digital forensics-related data is high but, to a certain extent, lacks validation from practitioners or applications in close-to-real investigative scenarios. Alternatively, visualisations focus towards on creating visual dashboards that are oriented towards statistics (e.g., the U.S. Department of Justice design document on creating dashboards[184]). Other examples of existing visual interfaces include interfaces such as the MITRE ATT&CK Navigator[32] that provides useful overlays to visualise a TTPs of different threats or allows an investigator to create their own.

One of the main challenges that current work in visual intelligence aims to address is the overload in data faced by investigators during their investigation. This has and has continued to be recognised as a particular problem in digital forensics' investigations [185] starting from triage right [186] through to data exploration [187]. Carvalho recognised the challenge of building a case against a malware-related crime and, while primarily focused on the use of semantic technologies, including a comprehensive user interface, search and a query builder to support investigators in interrogating their data [188]. Visualisations can also be utilised within user interfaces for LEAs to support the understanding of AI models, thus also enhancing explainability and transparency [189].

3.4.9 Use of artificial intelligence to support cybercrime investigations

One of the challenges faced by investigators into cybercrime operations is the increasing volume and variety of data to manage, interpret and analyse during an investigation, alongside understanding how this information all links together. There has been extensive research into the use of predictive and analytical methods to better support investigators across the entire investigation process to accelerate their approach. Typically, in the area of cybercrime, there is more text (or code) -based input than in other investigations, which may acquire significant amounts of visual media. Therefore, analysis around cybercrime investigations have the opportunity to be streamlined using AI.

As described by Europol, AI has the potential to completely transform policing operations [190], albeit with the need for extensive and effective safeguards and guardrails to be in place. As we have described in the previous sections there are opportunities for enhanced data analysis across information acquired from the dark web and through OSINT, for the analysis of ransom notes, to support malware and other code analysis, for rapid correlation of information across data collected in relation to cryptocurrencies or cyber threat intelligence or ultimately to offer decision support to investigators by bringing all this information together.

Areas where AI has already been identified as capable of supporting and enhancing cybercrime investigations are found throughout the entire investigation cycle. Starting from the automation of digital forensics processes [191], the extraction of metadata [192] and the use of LLMs to analyse long chat messages rapidly and extract relevant information [193]. Furthermore, AI has also been used to help structure information more effectively [194]. In fact, Kaur, Gabrijelčič and Klobučar [195] have extensively reviewed the opportunities for AI in cybersecurity with many of the same areas directly applicable to law enforcement activities as well. Furthermore, they pinpointed opportunities for future

[31] https://www.microsoft.com/en-us/power-platform/products/power-bi

[32] MITRE ATT&CK® Navigator https://mitre-attack.github.io/attack-navigator/

developments which included real-time identification of risk indictors, detection of new attacks, better predictive intelligence, multilingual considerations, triage, and analysis of breach data, amongst others.

3.4.10 Chain of evidence and evidential integrity

As discussed in the section focusing on standards, cybercrime and online investigations must ensure that they follow and adhere to proper procedures during intelligence and evidence collection to maintain evidential integrity and the chain of custody. This is a particular challenge for cybercrime investigations were collecting and processing information from online services, devices, networks and other sources and combining it with analytical products and processes often needs to be quick, and there may only be a single opportunity to capture such information. Investigators also need to make decisions about the specific tools they are using and whether they are suitable for use, and while may other considerations come into play, understanding the data provenance associated with any tool is essential [196].

One of the approaches that investigators should consider at the start of their investigation is their strategy for digital evidence [197]; this is essential for ensuring that any information that is collected is considered admissible at a later date, although it is also important to not over-collect information. Furthermore, utilising a standardised model that conforms with known approaches for digital evidence admissibility also helps to ensure evidential integrity throughout the investigative cycle [198].

Technology also plays an important role in cybercrime investigations; however, it also presents several challenges. Specifically, this includes 'challenges presented by computers to cybercrime investigations, including issues surrounding anonymisation, encryption, jurisdiction, caseloads, backlogs, data volume, eliciting data from electronic service providers, and the ever-changing technological landscape.'[199] Uses of evidence from AI-based systems also have to be carefully considered with additional validation to ensure accuracy and provenance [200]. These all have to be factored into chain of custody and evidential requirements, as well as the wider legal process.

3.5 Overview of legal considerations

Cybercrime is a multifaceted issue requiring the consolidation of numerous techniques to identify criminality and pursue lines of enquiry. While carrying out these activities, a number of regulatory matters must be considered to ensure individual rights are maintained. Core EU regulatory acts that relate to the pursuit of cyber-criminality include, but are not limited to, the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED), the Data Governance Act (DGA), the EU Data Act, and the EU Artificial Intelligence (AI) Act. While ENSEMBLE will directly address the core legal matters through task 2.6, here we provide an overview of the key pieces of relevant legislation.

a. General Data Protection Regulation (GDPR)

The GDPR is the EU's primary regulation for protecting personal data and regulating its processing. It applies to organizations within the EU as well as those outside the EU that offer goods or services to EU residents or monitor their behaviour. In pursuing cyber-criminality, LEAs must abide by provisions relating to 'consent', 'data minimisation', 'data subject rights', 'accountability', and 'data security'. Penalties for non-compliance with GDPR include significant fines that range up to €20 million or 4% of a company's global turnover (whichever is higher).

b. Law Enforcement Directive

The Law Enforcement Directive (LED) (Directive (EU) 2016/680) governs the processing of personal data by competent authorities for the purposes of prevention, investigation, detection, or prosecution of criminal offences and the execution of criminal penalties. The main objective of the LED is to ensure data protection when personal data is processed by law enforcement authorities. While law enforcement agencies require access to personal data to perform their duties effectively, this access must be balanced with individual rights. The directive harmonises national laws across EU member states, ensuring consistency while allowing some flexibility to accommodate specific national law enforcement practices.

The LED applies to the processing of personal data by police and criminal justice authorities, including public prosecutors and courts, for law enforcement purposes. The LED is based on principles relating to 'lawfulness, fairness, and transparency', 'purpose limitation', 'data minimization', and 'storage limitation'. The directive also grants individuals several rights, subject to limitations centred on the disclosure of information that could hinder investigations. Individual rights include the restricted right of access to personal data, the right to the rectification of inaccurate data, and the right to erasure or restriction of processing (in some cases). Member states may further restrict these rights to protect public or national security, or the rights and freedoms of others.

The LED allows for the transfer of personal data to third countries or international organisations, but only when the recipient offers an adequate level of data protection, or that specific safeguards (such as binding agreements or legal authorisations) are in place. The supervision and enforcement of the LED is governed by independent supervisory authorities designated by each EU Member State.

c. The Data Governance Act

The Data Governance Act (DGA) fosters the use of data in the EU while ensuring strong privacy protections, ethical usage, and the development of a fair and innovative data economy. The DGA is a cornerstone of the EU's broader digital strategy, aiming to establish a unified framework for data governance across the union. Its primary focus is to create oversight mechanisms that encourage the sharing, access, and use of data, while maintaining trust, security, respect for citizens' rights, and remain ethical and in compliance with privacy laws such as the General Data Protection Regulation (GDPR). One of its core objectives is to make data more accessible and usable by establishing clear rules and processes for data sharing between organisations, without compromising individual privacy and commercial interests.

d. The EU Data Act

The EU Data Act establishes rules regarding access to and use of data generated by Internet of Things (IoT) devices, cloud services, and other digital technologies. The Data Act allows public sector bodies to request access to privately held data in the event of exceptional need, such as during natural disasters, public health emergencies, or major security threats. In such cases, authorities may require access to real-time or historical data held by businesses (e.g. from IoT devices, logistics systems, or health platforms) to aid emergency response and coordination. This access is conditional upon the absence of timely alternative means of acquiring the data, the necessity and proportionality of the request, and strict use limitations tied to the specific emergency. The Data Act also permits data sharing with law enforcement or public bodies for clearly defined public interest purposes, such as

preventing crime, enforcing regulations, or ensuring public safety. However, requests must be justified, limited in scope, and subject to oversight.

The EU Data Act and the EU Data Governance Act introduce frameworks that have the potential to significantly impact how law enforcement agencies in the EU access, manage, and utilise data for their operations, from preventing crime to investigating and prosecuting illegal activities.

e. The AI Act

The EU Artificial Intelligence Act (AI Act) is the primary EU regulatory framework aimed at regulating artificial intelligence in a way that ensures safety, fundamental rights, and trust, while fostering innovation. The regulation takes a risk-based approach, classifying AI systems into four risk categories: unacceptable risk, high risk, limited risk, and minimal risk. Each level carries different regulatory obligations. The Act imposes differing obligations on developers and deployers based on the risk analysis. AI providers will be required to register high-risk systems in an EU-wide public database, while imposing a series of compliance requirements on both developers and deployers. These include 'risk management and quality control', 'robust data sets', 'clear documentation', 'human oversight', and 'security, accuracy, and performance monitoring'. The AI Act establishes both national and EU-wide regulatory bodies to monitor compliance. Each EU member state must appoint a national supervisory authority, while a European AI Office within the European Commission will coordinate enforcement and provide guidance. Non-compliance with the Act can result in significant fines—up to €35 million or 7% of a company's global turnover, depending on the severity of the breach.

In ENSEMBLE, T2.4 is carrying out an extensive legal and ethical analysis in relation to the project; therefore, the above provides an overview of the main areas under consideration.

3.6 Conclusions and next steps

In this section, we have provided an overview of the current state of the cybercrime investigation process for ransomware and unauthorised access to data and information, as well as reviewing the investigative needs and current capabilities for law enforcement in the key areas of cybercrime investigation. Specifically, we have focused on the key areas for ENSEMBLE to incorporate for enhancing cybercrime investigations including dark web, OSINT, cryptocurrencies, cyber threat intelligence, malware investigation, access to data, visualisation and chain of evidence. As this task progresses, we will focus on developing these into best practices in each of these areas, while also identifying potential future needs to inform the work on the cybercrime investigation roadmap later in the project. Furthermore, this review has also provided a solid foundation for the next phase of the project, which looks at the specific needs and operational practices of practitioners, exemplar use case scenarios and ultimately into the user requirements for the ENSEMBLE project.

4 ENSEMBLE user-centric methodology

ENSEMBLE is designed around an approach where practitioners, researchers, technology providers and legal experts work closely together to enhance law enforcement's approach and response to cybercrime investigation. The section outlines the approach and methodology for this collaboration, ensuring the successful execution of the project.

The methodology adopted by ENSEMBLE for the identification of user needs, expectations, use cases, and system requirements is firmly grounded in a user-centric approach, with particular focus on the operational context of European law enforcement agencies (LEAs) engaged in cybercrime investigations. By placing end-users at the centre of the design and development process, the project seeks to ensure that its outputs are not only technically robust but also aligned with the concrete needs and priorities of practitioners working to combat cybercrime.

This approach is motivated by the recognition that meaningful innovation in this domain must be informed by a clear understanding of real-world investigative workflows, challenges, and constraints. Accordingly, the methodology entails systematic engagement with LEA representatives through targeted consultations, structured feedback loops, and iterative validation exercises. These activities are designed to elicit operationally relevant insights that guide the definition of use cases and the specification of functional and non-functional requirements.

By continuously involving end-users throughout the project lifecycle, the methodology ensures that the developed tools and solutions remain fit for purpose, context-aware, and readily deployable in law enforcement environments. The following section outlines in detail how this user-centric approach has been implemented. In ENSEMBLE, end-users and practitioners are defined as law enforcement agencies such as police or gendarmerie units that are specialised in cybercrime cases. The project LEAs are comprised of:

- The French anti-cybercrime office (OFAC), which includes a unit specialising in ransomware attacks;
- The Directorate of Services for Innovation and Development of the Portuguese Ministry of Justice
- The Intelligence Service and the Technology Innovation Office of the Guardia Civil of Spain;
- The Department of Project Management of the General Police inspectorate of the Ministry of Internal Affairs of the Republic of Moldova;
- The General Directorate of Bucharest Police.

The three main phases employed within ENSEMBLE during this first period of the project have been:

1. Design and development of an **end-user survey** to help establish the current operating environment of the ENSEMBLE end-users and their approaches to investigating cybercrime.
2. Iterative development and analysis of **use cases (UCs) and use case scenarios** with feedback from across the consortium and several workshops with end users to enhance and concretise the use cases and use case scenarios in an operational setting.
3. Elicitation and prioritisation of **user requirements** aligned with the UCs, scenarios and the proposed technological scope of the project.

Each of these stages are described in more detail in the rest of this section.

4.1 Survey on end-users' needs and expectations

Considering the diverse array and number of stakeholders identified within the project, it was decided that employing an online survey would be the most appropriate initial method to comprehensively collect and discern their multifaceted needs around cybercrime investigation. The selection of the EU Survey platform was made on the basis of its user-friendly interface, compliance with the GDPR, and its widespread acceptance and utilisation within the European research community.

The ENSEMBLE project launched the online survey between March 7 and April 4, 2025, to gather insights from law enforcement agencies and cybercrime professionals about their operational needs, challenges, and expectations in combating cybercrime. The survey, shared via the EUSurvey platform, focused on three main cybercrime areas: ransomware attacks, cyber fraud and data theft, and unauthorised access to data, which aligned with the proposed UCs within ENSEMBLE. Its overall aim was to capture current investigative practices and observed shortcomings, training needs and overall expectations towards the project with the ambition to inform the development of AI-driven investigative tools and practical training resources. To ensure the success of this project and to produce meaningful and operational outputs, it is fundamental that the offered capabilities of ENSEMBLE meet the end-user's needs; therefore, the survey was designed to provide a solid foundation for this approach.

The questionnaire was structured in three sections, covering participant background, detailed questions on investigative practices and training needs, and final formalities such as exchanging contact details for those who would agree to be contacted again and thanking them. Responses from six project partners were collected to ensure the outcomes align with real-world requirements in cybercrime investigation and prevention. The responses collected through the survey directly inform the construction of the use cases, guide the training methods developed within WP6 of the project and help define user requirements for the development of the tools.

The results of this survey were subsequently transcribed into an Excel spreadsheet in order to conduct both a quantitative analysis and a qualitative analysis based on the open-ended responses provided by the participants. The results of the survey are presented in Section 5.

4.2 Approach towards defining the Use Cases

The second phase of ENSEMBLE's user-centric methodology focused on the development of the three Pilot Use Cases (PUCs), which followed a structured and collaborative methodology designed to ensure consistency and operational relevance. A standardised template initially drafted by CENTRIC and refined by ENSP was created to guide scenario construction across all use cases. This template, shared via the project's SharePoint, included two key sections: the current investigative landscape ("AS-IS") and the envisioned improvements using ENSEMBLE tools ("TO-BE"). Partners were invited to review and contribute to the template to ensure alignment across scenarios. Scenario leaders (ENSP for PUC1 and D.G.P.M.B. for PUC2 and PUC3) were responsible for completing the templates, with support from technical partners who detailed the investigative steps, technologies used, and data involved. The process included clearly defined deadlines, collaborative feedback periods, and a finalisation phase. To validate and refine the scenarios, dedicated online workshops were held, where law enforcement,

technical, and academic participants worked together to adapt the scenarios, assess investigative challenges, and ensure that the proposed tools responded to real operational needs. This methodology ensured that the PUCs were not only technically sound but also grounded in the investigative realities faced by end-users.

4.3 Methodology for the definition of user requirements

The PUCs are directly linked to the user requirements. Based on the various steps of the investigative process defined by the LEAs, and the tools proposed by the technical partners of the ENSEMBLE project to support these investigations, the user requirements were then formulated accordingly. This enabled direct and structured collaboration between the technical partners and the LEAs, ensuring the most effective and relevant outcomes for the project.

To effectively classify the user requirements gathered from Law Enforcement Agencies (LEAs) within the ENSEMBLE project, the MoSCoW prioritisation methodology was adopted. This well-established technique categorises requirements into four levels: “Must have”, “Should have”, “Could have”, and “Won’t have”; based on their criticality to the project’s success and their alignment with the project’s scope. Its use is particularly relevant in European collaborative contexts, as it fosters a shared understanding among diverse stakeholders, supports resource optimisation, and enables agile, iterative development.

To collect these requirements, a structured table was distributed to all participating LEAs. The table is accompanied by detailed instructions and guidance to ensure clarity and consistency in responses. It defines what a user requirement is and provides tips for writing effective entries, such as focusing on user needs, avoiding ambiguity, and ensuring measurability. Each row in the table captures a single requirement and includes fields such as ID, type (functional or non-functional), origin, related use case and step, main actor, description, data involved, MoSCoW priority, comments, linked work package, and validation status. This approach ensures that user needs are captured in a clear, actionable, and prioritised manner to guide the project's technical development.

Building on this foundation, the compiled list of requirements underwent a collaborative review process with technical partners such as VICOM, CERTH, BYRON, TREE, ENG, CFLW, and CEA. Facilitating open communication and feedback sessions, this stage sought to align end-user expectations with technical perspectives, enriching the initial requirements with valuable insights and expertise. The integration of feedback from technical partners led to the finalisation of a comprehensive set of requirements, extending across security considerations, operational needs, and communication requirements. This iterative and inclusive methodology ensures a seamless alignment between end-user expectations and the technical capabilities and insights, laying a robust foundation for the subsequent phases of the ENSEMBLE project. The list of requirements can be accessed in Section 0.

5 Analysis of end-users and practitioners' needs

The ENSEMBLE partners decided to conduct an online survey to gather the needs of end-users and practitioners in the domain of cybercrime investigation. This survey directly contributed to T2.2: "User-centric creation, analysis, and definition of use cases and requirements", led by ENSP. The survey laid the foundation for the enhancement of the use cases and elicitation of the user requirements to follow.

The following section presents the survey, its objectives and structure, followed by public summary of analysis of the results and outcomes that emerge. These results help ENSEMBLE in completing an in-depth analysis in identifying the needs and requirements of end-users in the fight against cybercrime.

5.1 Survey objective and presentation

The online survey called "End-user survey on identifying the operational needs of police forces and practitioners for the detection, fight and prevention of cybercrime" was published via the EUSurvey platform.

5.1.1 Objective of the ENSEMBLE survey

The main objective of this survey is to collect valuable insights from end-users such as LEAs and cybercrime practitioners regarding their operational needs, investigative challenges, and expectations in the field of cybercrime investigation, for the prevention and disruption of cybercrime.

The following specific objectives of this survey have been identified and are to:

- Identify **real-world operational challenges** faced in combating cybercrime.
- Understand **investigative practices** across various regions and organisational contexts.
- Gather feedback on **tools**, **training needs**, and **collaboration frameworks**.
- Inform the design of **AI-driven investigative tools and methodologies**.
- Ensure that ENSEMBLE delivers **practical and relevant outcomes** for day-to-day cybercrime investigation operations.

The six end-user focused partners of the ENSEMBLE project were asked to respond to the questionnaire (GPI, PJ, ENSP, RAD, GUCI, and D.G.P.M.B). A minimum of five responses per partner was requested to obtain a sufficient number of results for a representative analysis of the needs and requirements of end-users. ENSEMBLE end-users were therefore encouraged to disseminate the survey within their units to gather a total of five responses.

The survey's scope encompasses three major use cases that are at the core of contemporary cybercrime activities.

- The first use case focuses on ransomware attacks and delves into the growing prevalence and evolving nature of ransomware incidents. It examines how these attacks have developed over time, the tactics used by malicious actors, and the increasing sophistication of ransomware variants. Particular attention is given to the ongoing challenges organisations face in detecting and mitigating such attacks, especially given the rise of double extortion techniques and ransomware-as-a-service (RaaS) models.
- The second use case is based on Cyber Fraud and Data Theft. This use case focuses on the widespread issue of cyber-enabled financial fraud and the theft of sensitive data. It highlights the mechanisms used in online scams, phishing campaigns, and social engineering schemes

aimed at exploiting individuals and organisations for monetary gain. Additionally, it investigates the black-market trade of stolen personal and corporate data, emphasising the impact on both privacy and financial security.

- Finally, the third use case addressed by the ENSEMBLE project and highlighted in the survey concerns unauthorised access and data exploitation. The final section maps out the landscape of threat actors involved in gaining illicit access to digital systems and exploiting the data they extract. It explores the tools and techniques used to infiltrate networks, as well as the role of underground forums and marketplaces in facilitating the sale and distribution of compromised data. This use case provides insight into the broader cybercriminal ecosystem and its implications for cybersecurity resilience.

5.1.2 Overview and structure of the survey

The structure of the survey was designed to consolidate information about the use cases, to understand the needs of end-users and the difficulties encountered during their investigations, as well as their expectations regarding training, which also helps to support future work under WP6.

The survey was divided in three main sections. The first section, entitled “PARTICIPANT INFORMATION SHEET” recalls what the ENSEMBLE project consists of and what its aims are, then presents the survey and its objectives. At that point, participants are reminded of the conditions of participation in this survey, including their rights and the voluntary nature of their involvement in compliance with GDPR (General Data Protection Regulation). This section also contains the statement of informed consent.

The second part, simply titled "THE SURVEY", contains questions directly related to the core subject of the ENSEMBLE project. To structure this comprehensive set of questions, this section has been divided into four distinct parts.

General introductory questions

The first part, titled "GENERAL INTRODUCTORY QUESTIONS" consists of nine questions and aims to better understand the respondents’ profile as well as the nature of their work and the environment in which they operate. The questions were designed to collect general background information about the respondent’s professional role, organisational affiliation, and operational environment. It covers the type of law enforcement or expert institution they belong to, their specific role within a cybercrime unit, and the scope of their jurisdiction, whether local, national or international. The questions also explore the size and responsibilities of their team, involvement in cross-border cooperation, and the most commonly encountered types of cybercrime. This foundational information helped to contextualise the respondent’s insights inside the broader framework of the cybercrime landscape.

Specific subject-related questions

The second part, called "SPECIFIC SUBJECT-RELATED QUESTIONS", comprises 36 questions aimed at helping us better understand the project's end-users current capabilities and needs in terms of investigation practices and training

This second part is itself divided into 4 subsections, entitled: "A. INVESTIGATION"; "B. TRAINING"; "C. RISK INDICATORS & RED FLAGS" and "D. EXPECTATIONS TOWARDS ENSEMBLE".

This second section of the survey focuses on the practical aspects of cybercrime investigation, aiming to gain detailed insights into the methods, challenges, and operational realities faced by law

enforcement and expert units. It explores how investigations are initiated, who decides to launch them, and the technical and procedural difficulties encountered throughout the investigative process, from identifying and collecting data to producing court-admissible evidence. The section also assesses the types of data and tools used, the need for technological support, and cross-border cooperation challenges within the EU. In addition, it addresses current training practices and needs, competencies, and expectations regarding the ENSEMBLE project's upcoming training modules. Finally, it gathers input on risk indicators used to detect cyber threats and asks participants to express their specific expectations towards the ENSEMBLE project to ensure alignment between the project outputs and their operational needs.

Finally, the third major part of the survey is devoted to thanks and formalities such as the exchange of contact information in case of further questions to the research team.

In total, 21 respondents provided answers to the survey representing the six end-users organisations with five countries represented Spain, Portugal, France, Romania and Moldova.

The results were divided into give sections focused on different areas that can inform the future developments within ENSEMBLE:

1. Profiles and competencies of the survey respondents and their scope of work
    - A summary of the roles of the investigators, the type of unit they work in, whether they work primarily at the local or national level and the main cybercrimes encountered.
2. Investigation triggers and case initiation
    - A summary of how investigations are initiated within the unit they work, and the mechanisms associated with each of those triggers
3. Priorities and challenges in cybercrime investigations
    - A summary of the understanding of the key needs of each individual investigator and their unit alongside the current barriers and difficulties faced.
4. Tools and resources in current practice
    - A summary of the current tools used within the unit, issues faced when using them and needs for future tools with specific requirements.
5. Legal and cross-border obstacles
    - A summary of the legal challenges faced during investigations and the extent to which they face difficulties either with legal frameworks or for the exchange of data in the cross-border environment.

The results from each of these sections was then summarised and used to inform the development of the use cases, use case scenarios and user requirements. At a later stage, they will also help inform the training requirements.

6 Use Case Development

6.1 Approach

From the outset, ENSEMBLE has defined three Pilot Use Cases (PUCs) each tackling a different issue in the cybercrime investigation area. The first use case, led by ENSP, focused on ransomware and initially included a single scenario. ENSP subsequently added a second scenario to enrich the scope of the use case.

The second use case, entitled “Cyber fraud and data theft”, comprises three distinct scenarios. These address, respectively, data theft via watering hole attacks, data theft through fraudulent registration forms, and a case of financial fraud. This use case is coordinated by D.G.P.M.B., who played a central role in shaping its content and direction.

The third and final use case, “Data theft from unauthorised access”, includes two scenarios. The first explores the theft of multimedia content intended for sale on the dark web, while the second focuses on data theft for extortion purposes. As with the second use case, D.G.P.M.B. assumed leadership of both scenarios within this third domain.

The development of the PUCs followed a collaborative methodology. A standardised template was created to guide the structuring of each scenario, elaborating on the descriptions originally defined during the proposal phase. This template, initially drafted by CENTRIC and subsequently refined by ENSP, was shared to facilitate collective input from across the consortium. All partners were encouraged to review the document, suggest modifications, and provide comments to ensure consistency and comprehensiveness across the different scenarios.

This process was governed by a defined timeline. The preliminary version of the template was presented to all partners involved in Work Package 2 (WP2), and iterative rounds of feedback and updates were provided by partners, with all end-users encouraged to provide input and improvements based on their knowledge, expertise and ambitions for ENSEMBLE. Following the completion of the finalised version of the template was then shared and subsequently, the scenario leaders were responsible for populating the templates with the relevant information. Upon completion of this phase, technical partners were tasked with detailing the investigative steps and integrating appropriate tools to support the operational needs of investigators at each stage of the scenario lifecycle.

This template is designed as a foundational document for constructing a detailed use case within the ENSEMBLE project. The document is structured to guide contributors through two main sections: the current investigative reality (“AS-IS”) and the envisioned enhanced approach using ENSEMBLE tools (“TO-BE”).

6.1.1 “AS-IS” – Current investigative landscape

This section of the PUC template allows LEAs to describe the typical cybercrime activities they encounter in their investigation and to detail the different steps currently undertaken in their investigative approach. It aims to highlight investigative difficulties and operational pain points.

Several subsections are contained in the “AS-IS” description, namely:

- **Motivation:** In this section, the scenario lead details the reasoning behind the selection of the PUC scenario. Contributors are expected to explain the reasoning behind **of the selected cybercrime activity** as well as the **relevance and impact it has** in their country or organisation.
- **Scenario -title:** The scenario lead indicates here the detailed name (or type) of the cybercrime as well as the scale of the crimes involved
- **Scenario description and investigative steps:** LEAs have the possibility here to describe the **full storyline** of the attack: how the attack is launched, how the attack unfolds, its impact (data loss, financial and psychological damage), and a **general overview of the investigative process**.
- **Difficulties encountered:** Finally, LEAs can enumerate in this subsection the **challenges they typically face** during investigations.

6.1.2 "TO-BE" – Future-state enhanced by ENSEMBLE

This section details how ENSEMBLE tools and methodologies can complement and improve the investigative process employed by LEAs. The narrative is expanded into a step-by-step breakdown, linking current actions to enhanced technological interventions.

For each investigative step, LEAs provide:

- **Investigations actions:** A step-by-step breakdown of the investigative steps typically followed for the described cybercrime.
- **Technology used:** LEAs indicate here any potential technological tools or solutions currently used by their units during investigations. In a second step, ENSEMBLE technical partners are asked to add the information concerning the tools proposed to be developed within the project and the specific investigative steps where it is they could be most relevant and impactful (e.g. OSINT).
- **Data used:** Firstly, LEAs enter here the types of data used during each step and technical partners add the data necessary for the use of their tool (e.g. IP logs, email headers, crypto wallet addresses, etc.).
- **ENSEMBLE added-value:** Here, technical partners are expected to describe how ENSEMBLE technologies specifically improve a particular investigative step through the use of their tool (e.g. automated tracing, cross-border collaboration support, AI-driven detection). **Associated Key Results/Objectives (KRs/Os):** Finally, in this section, technical partners can link each step to the relevant project goals (e.g. "O3: Improved innovative tools for advanced and automated tracing of illicit crypto asset transactions").

6.1.3 Additional input and feedback

At the end of the template, contributors were able to insert any additional observations, clarifications, or suggestions relevant to the scenario or the ENSEMBLE approach.

6.1.4 Pilot use case workshops

As part of ENSEMBLE, under WP2, a series of three online workshops were organised to collaboratively refine each PUC scenarios. The primary objective of these workshops was to foster collaboration among law enforcement agencies, technical partners, and academic researchers, enabling the co-development of investigative scenarios grounded in operational realities. These workshops also

facilitated the direct integration of investigative tools, ensuring they met the practical needs of end-users.

Each PUC was addressed in a dedicated workshop, and every scenario within the PUCs was allocated approximately one hour. Preparatory tasks were essential: use case leaders were required to complete the “AS-IS” and key sections of the “TO-BE” templates, while technical partners had to document the technologies proposed, their benefits, and relevant knowledge requirements. All participants were expected to familiarise themselves with the materials in advance to contribute meaningfully to the discussions.

Workshops followed a structured format. Each session began with a presentation by the use case leader, who introduced the scenario and highlighted the investigative actions and data sources involved. Subsequently, technical partners demonstrated their tools, detailing their application to the scenario and outlining the expected operational benefits. The remainder of each session was dedicated to interactive discussion, during which templates were adjusted collaboratively in response to feedback, particularly from law enforcement participants.

The workshops were held via Microsoft Teams. The PUC2 and PUC3 sessions occurred on May 7th, 2025, and the PUC 1 session took place on May 12th, 2025. These workshops brought together a diverse group of 36–38 participants per session, representing technical, academic, and operational domains from multiple European countries.

The following partners attended these workshops: CERTH, VICOM, ENG, CFLW, IKN, BYRON, TREE, UL, ULIM, RAD, ENSP, PJ, GUCI, GPI, DGPMB, CYBERP, CENTRIC.

The workshops fostered extensive discussions on tool capabilities, data integration, and investigative strategies. Feedback gathered during the sessions informed the development of a consolidated operational framework for ENSEMBLE, with a focus on ensuring interoperability and enhancing investigative support across PUCs.

A report of these three workshops was designed and published on the project prepared and shared with all partners. Across the three workshops, participants raised a wide range of points that cut across technical, procedural, and methodological issues. The discussions frequently focused on usability, interoperability, and integration issues concerning the tools presented. Specific attention was given to how well these tools could be accessed by different stakeholders, how intuitive they were to use, and whether they were suitable for real-world investigative environments.

Another recurrent theme involved data management and standardisation. Participants questioned whether the data formats employed by the various tools were compatible and whether there was sufficient standardisation to allow seamless integration. These reflections were often aimed at improving cross-tool communication and preventing workflow fragmentation.

Concerns were also expressed about taxonomy alignment, with discussions touching on the potential inconsistencies between the classification systems used by different tools and how well they aligned with European Union standards. This issue reflected a broader interest in ensuring conceptual and semantic coherence across all technical and operational components of the project.

In terms of tool interaction, the workshops included discussions on technical interoperability, especially between AI-based tools, such as those using natural language processing or cross-modal analysis. Participants explored how these technologies could be synchronised for more efficient and accurate evidence analysis.

Operational discussions also dealt with workflow optimisation. There was a strong focus on how the scenarios and the tools could be used to refine investigative strategies, particularly in relation to different types of cybercrime. Questions were raised about which tool combinations were most effective for specific cases and how workflows might need to be adjusted based on practical feedback.

In addition, data volume and processing capacity emerged as a concern. Some participants noted the limitations of current tools in handling large-scale datasets, and emphasised the need for more robust data processing protocols and infrastructure.

Finally, several points addressed the methodological evolution of the project, such as the refinement of use case templates and the incorporation of workshop feedback into upcoming deliverables.

To conclude, the workshops fostered extensive discussions on tool capabilities, data integration, and investigative strategies. Feedback gathered during the sessions informed the development of a consolidated operational framework for ENSEMBLE, with a focus on ensuring interoperability and enhancing investigative support across PUCs.

6.2 Summary of the Pilot Use Cases

6.2.1 PUC1 – Ransomware

The first PUC is led by ENSP and focused on different aspects of ransomware attacks. As we have seen from Section 2, ransomware continues to be a major threat to individuals and organisations across Europe and cases are continuing to increase. For PUC2, there are two different ransomware scenarios that each require different scales of investigation.

Scenario 1: Small-scale attack of ransomware with one attacker and one victim

The perpetrator in this ransomware attack is a student at an engineering school. The motivation for the attack is unknown. The targeted victim is a small local company, called “2Cs Inc.”. It is unknown how the student infiltrated the network of 2Cs Inc. or what kind of payload delivery method was used. The evidence gathered by local law enforcement consisted of a simple ransom note found on the company's laptops. From initial investigations, it appears that the ransomware and note was not developed by the student themself but found online.

The ransom note contains a crypto address, left by the attacker, requesting the payment of 150$ in Bitcoin, which 2Cs Inc. has refused to pay. Following the request for payment of the ransom, 2Cs Inc. makes a complaint at the police station.

In the proposed scenario, law enforcement takes up the investigation applying various investigative techniques that include cryptocurrency analysis, open-source intelligence and dark web monitoring, use of CTI, malware analysis of the ransomware, multimodal data processing, decision support tools and visualisation to identify the mechanism of attack and the attacker. The proposed investigation process is divided into 31 different investigative steps.

Scenario 2: Large-scale ransomware attack with approximately 20 attackers and 50 victims (Ransomware-as-a-Service)

Since 2020, French companies have been victims of a ransomware named “NeuroCrypt” (fictional name). It was soon discovered that the types of victims targeted were extremely varied, ranging from

small businesses such as restaurants and farm stores to medium-sized companies with more than 50 employees.

This was the first indication that the attackers behind NeuroCrypt were not following a clear-cut attack policy. In the ransom notes and attacking IP addresses, it was possible to observe many differences and variations in their operating methods. Open-source research identified that different attackers were using the same ransomware, indicating that this was indeed a RaaS (ransomware as a service) model.

In total, almost 50 French victims of this ransomware have been counted, involving a large number of different attackers. Some arrests were made, but the creator of distributor of the organisation behind the ransomware and their many affiliates have not yet been identified.

In the proposed scenario, law enforcement takes up the investigation applying various investigative techniques that include cryptocurrency analysis, open-source intelligence and dark web monitoring – and the correlation of such data, use of CTI, malware analysis of the ransomware, multimodal data processing, decision support tools, querying and visualisation to identify how the different attacks are linked. The proposed investigation process is divided into 30 different investigative steps.

6.2.2 PUC2 – Cyber fraud and data theft

The second use case is led by DGPMB and focuses on three different aspects of cyber fraud and particularly data theft. As we saw with PUC1, PUC2 also represents a widespread problem across Europe and not one that is localised to Bucharest.

Scenario 1: Data theft via watering hole attack

Cyber fraud is an umbrella term that covers a wide range of illegal activities carried out through technology, particularly the internet and digital systems, with the aim of obtaining money, personal data, or unauthorised access to data or information systems.

In this context, we address investment and cryptocurrency fraud, due to the growing number of victims reported in recent years. These types of fraud typically involve false promises of quick profits through online investments, fake cryptocurrency trading platforms, or participation in digitally disguised pyramid schemes. The victims are generally individuals who, lured by the prospect of fast and guaranteed returns, transfer significant sums of money to accounts controlled by international criminal groups.

The scenario focuses on a prevalent form of digital fraud: deception via online classified platforms such as OLX. This modus operandi involves the exploitation of users' trust in legitimate commercial websites and mirrors the operational logic of watering hole attacks commonly seen in cybersecurity.

Similar to watering hole tactics, the perpetrators do not directly compromise the victim's infrastructure, but instead infiltrate the digital ecosystem frequented by the target—in this case, online marketplaces. By establishing apparently legitimate interactions (e.g., simulated sales or fake delivery arrangements), cybercriminals redirect users to fraudulent websites impersonating banking institutions or courier services. These spoofed pages are used to harvest personally identifiable information (PII) and financial credentials.

This type of fraud aims at unauthorised data acquisition, with the primary objective of committing identity theft or financial theft. The method leverages predictable user behaviour and the perceived

credibility of known platforms, underlining the critical need for enhanced preventive cybersecurity measures, public awareness campaigns, and the implementation of robust technical safeguards by both users and service providers.

The investigation includes the forensic analysis of artifacts from the compromised platform, analysis of the platforms content, OSINT activity, tracing of cryptocurrencies, the use and sharing of cyber threat intelligence, secure storage of the evidence, decision support tools including reporting and visualisation. The scenario is divided into 24 different investigative steps.

Scenario 2 – Data theft via fake registration form

The scenario builds on many of the features of the first PUC2 scenario, but focuses towards the kind of fraud that typically involves false promises of quick profits through online investments, fake cryptocurrency trading platforms, or participation in digitally disguised pyramid schemes.

Specifically, data theft through fraudulent update forms—delivered via email or SMS—has become a prevalent and evolving form of cyber-enabled fraud, relying heavily on phishing and social engineering techniques.

The typical modus operandi involves the distribution of deceptive messages that appear to originate from trusted institutions such as banks, telecommunications providers, courier companies, or public authorities. These messages urge recipients to “update account information” or “verify identity” to avoid service suspension or account deactivation. The included phishing links redirect users to spoofed websites that closely resemble the interface of the legitimate entity. Once the victim completes the form, sensitive personal and financial data—including national identification numbers (CNP), IBANs, card numbers, login credentials, and two-factor authentication codes—are harvested in real-time by the attackers.

This attack vector has significantly expanded amid the widespread digitalisation of services and the increasing reliance on online platforms. Perpetrators often remain anonymous by using VPNs, temporary hosting infrastructure, burner domains, and prepaid SIM cards. While any internet user can be targeted, vulnerable demographics with lower digital literacy are particularly at risk.

The investigation includes the forensic analysis of artifacts from the compromised registration (or similar) form, analysis of the platforms content, OSINT activity, tracing of cryptocurrencies, the use and sharing of cyber threat intelligence and the correlation of multiple incoming data streams, secure storage of the evidence, decision support tools including reporting and visualisation. The scenario is divided into 21 different investigative steps.

Scenario 3 – Financial fraud

This scenario builds on the first two scenarios but focuses more specifically on fraud. In recent incidents, perpetrators have leveraged social media platforms to promote paid advertisements targeting specific demographic groups—most notably individuals aged 65 and above. It is presumed that filtering tools were used to isolate this vulnerable segment of the population.

Once the target audience is identified, the attackers deploy deepfake technology to fabricate video materials in which well-known public figures appear to endorse "fast-track" financial gain opportunities. These manipulated clips are used to establish trust and credibility, prompting victims to submit their personal identification details (name, phone number, email) through online forms.

Following this initial data capture, victims are contacted via VOIP calls from spoofed phone numbers—simulating official institutions or trusted entities. They are then encouraged to migrate the conversation to encrypted messaging platforms such as WhatsApp, Signal, or Telegram, which support file transfers, screen sharing, and URL hyperlink access.

Using advanced social engineering tactics, the attackers guide victims to access fraudulent websites designed to closely imitate legitimate investment platforms. The malicious actors update these platforms in real time to reflect false investment returns, thereby reinforcing the illusion of legitimacy with every transfer made by the victim.

Victims are further manipulated into installing remote access tools (such as AnyDesk or TeamViewer), allowing the attackers to gain direct control over their mobile devices and, by extension, their online banking applications. This unauthorised access facilitates illicit fund transfers without the victim's consent or knowledge.

The investigation includes the forensic analysis compromised web pages, analysis of the platforms content, OSINT activity, tracing of cryptocurrencies, the use and sharing of cyber threat intelligence and the correlation of multiple incoming data streams, secure storage of the evidence, decision support tools including reporting and visualisation. The scenario is divided into 22 different investigative steps.

6.2.3 PUC3 – Data theft from unauthorised access

The third use case is also led by DGPMB and focuses on two different aspects of financial fraud, data theft and exploitation of that data. As we saw with PUC1 and PUC2, PUC3 also represents a widespread problem across Europe and not one that is localised to Romania.

Scenario 1: Data theft of multimedia to be sold on the dark web and exploitation of system resources with crypto-jacking

In the current cybercrime landscape, unauthorised access to information systems has become a gateway to large-scale data exfiltration, driven by the rapid expansion of underground digital marketplaces. These illicit platforms facilitate the monetisation of stolen personal and institutional data, enabling perpetrators to profit from sensitive information with minimal operational risk and high anonymity.

This criminal phenomenon poses significant threats to both public and private sector entities, as well as to individual citizens, including sextortion schemes, where offenders leverage unlawfully obtained personal media files and communications to blackmail or intimidate victims. Such cases underline the psychological and reputational harm suffered by victims, in addition to potential financial losses.

In this scenario, an unidentified threat actor is planning to launch a cyber-attack against a well-known private company. Initially, the attackers extracted data from social media to gather information about company employees, their roles and responsibilities. Using the information gathered, the attackers chose an executive employee to impersonate.

A spearphishing email, fraudulently impersonating the company's executive employee, was delivered to the victim which contained an attached malicious excel file, disguised as a pivot table to convince the victim to open the file. In the background, a Remote Code Execution vulnerability was exploited to download and execute an EXE file on the victim's workstation. A PowerShell code was executed to

disable real-time protection software, to maintain persistence and to drop a Remote Access Trojan (RAT) payload.

Once running, the malware collects basic information from the victim's workstation and sends it, using an encrypted TCP tunnel, to a command and control (C&C) server to register that the victim's device is online and ready for control.

As the infected endpoint is part of an enterprise network, the malware begins automated network reconnaissance to identify other reachable hosts. The attacker, exploring the network with unprivileged access, identifies a shared network location containing multimedia archives used during business processes such as employee onboarding, identity verification, or client intake.

The malware escalates privileges to gain higher-level permissions, allowing access to restricted folders and bypassing security controls. The stolen multimedia content is then compressed, encrypted, and exfiltrated through a secure, often anonymized, channel — typically a VPN or Tor-based relay — to infrastructure controlled by the attacker.

Subsequently, the stolen media is advertised and sold on Dark Web marketplaces and illicit forums, targeting buyers interested in identity fraud, forgery services, or account takeovers.

The investigation includes the acquisition and analysis of the initial data collected, the analysis of the platforms content, OSINT activity, tracing of cryptocurrencies, the use and sharing of cyber threat intelligence, malware analysis and the correlation of multiple incoming data streams, secure storage of the evidence, decision support tools including reporting and visualisation. The scenario is divided into 25 different investigative steps.

Scenario 2 – Data theft for extortion

Extortion is increasingly driven by theft of sensitive data through unauthorized system access, shifting from selling data to using it for intimidation. The threat of exposure causes significant emotional and reputational stress on victims.

In cybercrimes, perpetrators exploit digital weak points to access valuable data like personal media, identity documents, business records, confidential files, and private communications. This stolen data fuels extortion campaigns, where victims, individuals or organisations are threatened with public exposure unless they pay. Threats are often issued via anonymous websites with countdown timers or through direct messages and emails showing stolen content to intimidate and coerce compliance.

The harm caused by these cybercrimes goes well beyond financial loss, including emotional trauma, and damage to their reputation, as well as legal concerns. The fear of potential exposure can lead to long-lasting distress and loss of trust in digital systems and affect wider family members, colleagues, or entire organisations, amplifying the harm.

Perpetrators plan operations carefully, using anonymous hosting, decentralised DNS, and bulletproof providers to publish extortion sites. They communicate via encrypted apps and rogue email servers registered abroad. Extorted payments are demanded in cryptocurrencies, using mixers and chain hopping to obscure money trails. The cross-border nature complicates evidence gathering, as data is spread across multiple jurisdictions, cloud services, and anonymised platforms.

This scenario follows a sophisticated cyber extortion campaign that targets a major financial institution through a multi-stage, technically complex operation. The perpetrators initiate their attack by

exploiting an unpatched vulnerability in the institution's public-facing web server. Afterwards, they deploy a web shell that enables remote command execution and extracts sensitive information.

Afterwards, the perpetrators establish an anonymous website hosted on a server in a foreign jurisdiction, with a countdown timer for the release of the data, designed for psychological extortion and high visibility across underground forums and the dark web to maximise reputational and financial pressure. In parallel, the attackers employ rogue email servers, also hosted across multiple jurisdictions, to deliver direct extortion messages to key executives and decision-makers. These emails contain selected excerpts of the stolen data as proof of compromise, articulate financial demands via cryptocurrency, and threaten full public exposure upon non-compliance. The attackers further obscure their infrastructure by employing bulletproof hosting, domain fronting, and anonymisation networks, complicating traditional attribution efforts.

The investigation includes the acquisition and analysis of the initial data collected and forensic analysis of the intrusion, the analysis of the platform's content, OSINT activity, tracing of cryptocurrencies, the use and sharing of cyber threat intelligence, malware analysis and the correlation of multiple incoming data streams, secure storage of the evidence, decision support tools including reporting and visualisation. The scenario is divided into 23 different investigative steps, including elements of cross-border investigations.

7 User Requirements

The extensive descriptions of the PUCs then lay the foundation for describing each of the user requirements for the system. This final step in this first phase of the project allows for clear definitions and expectations of what is expected of ENSEMBLE from the end users.

7.1 Approach to requirements extraction

7.1.1 Objective and methodology

The method used to collect user requirements was to create a table that was sent to all ENSEMBLE LEAs so that they could complete it and submit it to ENSP with their specific needs and requirements.

The user requirements table is designed to collect structured and meaningful input from project stakeholders. The sheet provides both a conceptual explanation of what user requirements are and detailed guidance for completing each field of the table.

The document opens by defining a user requirement as a statement describing a specific need or expectation from end-users, which the project's system or solution must fulfil. It emphasises that such requirements are crucial in shaping the system's design, development, and evaluation phases. They should be clear, user-centred, and framed in a way that can be easily understood and verified.

The template offers practical tips to help contributors write effective user requirements. These include:

- Expressing the requirement from the user's point of view, focusing on what the user needs to achieve.
- Avoiding ambiguous or overly technical language.
- Keeping statements simple, specific, and measurable.
- Ensuring that each requirement can be tested or validated later in the project.
- Being concrete about what the system should do, rather than how it should do it.

These tips are meant to improve the consistency and quality of user contributions, especially when multiple organisations or countries are involved.

Each row in the user requirements table corresponds to a single requirement. The following fields must be completed, each accompanied by its own set of instructions:

1. **ID**: An identification number or code to uniquely label each requirement.
2. **Requirement Type**: Indicate whether the requirement is *Functional (F)* or *Non-functional (NF)*. Functional requirements describe what the system should do (e.g. features or use cases), while non-functional requirements refer to performance, usability, reliability, etc.
3. **Source / Origin**: Specify where the requirement comes from—this could be a grant agreement, a stakeholder interview, a workshop, a use case, or other forms of user input.
4. **Use Case #**: If applicable, refer to the corresponding use case number that this requirement is derived from.

5. **Scenario #**: If applicable, refer to the corresponding scenario number that this requirement is derived from.
6. **Step #**: If the requirement refers to a specific step within a use case, indicate the number of that step.
7. **Main Actor**: Identify the role of the user or stakeholder associated with the requirement (e.g. analyst, investigator, team leader).
8. **Requirement Description**: Provide a clear and detailed description of the requirement. For example: "The system should allow investigators to filter search results by date and location."
9. **Data Needed or Used**: Describe any specific data that is needed, referenced, or processed by the functionality (e.g. network logs, reports, structured datasets).
10. **MoSCoW Priority**: Assign a priority level using the MoSCoW method:
    - *Must have*: Essential for the system to function.
    - *Should have*: Important but not critical.
    - *Could have*: Nice to have if time and resources allow.
    - *Won't have (this time)*: Explicitly excluded from the current version.
11. **Comments**: Use this field to add clarifications, identify open questions, or mention any uncertainties or risks related to the requirement.
12. **Linked WP / Task**: Indicate the related Work Package or Task within the project, if relevant.
13. **User Validation**: Note whether the requirement has already been validated by users or still needs to be. This field supports iterative development and tracking of stakeholder approval.

7.1.2 MoSCoW prioritisation methodology

To best classify the user requirements established by the LEAs within the framework of the ENSEMBLE project, the MoSCoW method was chosen. The MoSCoW prioritisation methodology is a well-established technique used in project management and business analysis to classify and prioritise requirements based on their importance. The term "MoSCoW" is an acronym representing four categories of priority:

- ✓ **Must have:** These requirements are essential to the success of the project. Their absence would render the solution unworkable or the project incomplete.
- ✓ **Should have:** These are important but not critical. While they add significant value, the project can still be considered successful without them, at least in the short term.
- ✓ **Could have:** These are desirable enhancements that can be included if time and resources permit, but they are not necessary for the core functionality.
- ✓ **Won't have (this time):** These elements are explicitly excluded from the current scope but may be considered for future phases or developments.

This method proves particularly valuable in the context of European collaborative projects, which typically involve multiple stakeholders across different countries, disciplines, and organisational cultures. The application of the MoSCoW technique offers several key benefits.

The MoSCoW methodology contributes significantly to the success of collaborative projects by establishing a common understanding among stakeholders of what is considered critical versus optional, thereby enhancing communication and reducing ambiguity. It also facilitates consensus-building, which is particularly valuable in multidisciplinary and international teams where priorities may naturally diverge. By focusing efforts on delivering the most essential requirements first, the method ensures the effective allocation of limited resources such as time, budget, and personnel. Moreover, it strengthens risk management by guaranteeing the early delivery of core functionalities, which are crucial to the viability of the project. Finally, the approach supports iterative and agile development models, often preferred in European project frameworks, by allowing priorities to be adapted flexibly as the project progresses.

It is worth noting that there are minimal number of requirements that have a must/could/should rating that are currently out of scope for the originally foreseen ENSEMBLE toolkit. During the development of the technical requirements and the continued evolution of project, these requirements will stay under review and where practical and feasible ENSEMBLE will make every effort to incorporate open-source tools into the pipeline and/or identify existing tools within the ENSEMBLE toolkit that could support further developments in this area.

7.2 User Requirements

The user requirements were collected and mapped according to the process described above. In total, 109 initial user requirements have been established, 103 of which are functional requirements and 6 of which are non-functional requirements. The requirements are distributed across the three use cases and seven different scenarios, with many requirements being applicable in multiple use cases and multiple scenarios. Currently, all tools expected to be developed, enhanced or customised within ENSEMBLE are represented within the UR, and their specifications will be further elaborated under T5.5 on technical specifications.

8 Conclusions and next steps

This deliverable has provided an overview of the initial cybercrime landscape, the results of the end-user survey, the initial version of the use cases and use case scenarios, and the first version of the user requirements. The inputs to this deliverable are the results of two tasks T2.1 Identification and analysis of International and European best practices of cybercrime investigation methodologies and T2.2 User centric creation, analysis, and definition of use cases and requirements. Both of these tasks will continue to be active for the next 16 months until the submission of the second version of this deliverable. Therefore, especially for the use cases and user requirements, we consider these as living documents that will continue to be refined and updated in line with the project's progress and the ever-evolving cybercrime landscape.

Specifically, regarding T2.1, in this deliverable we have focused on information in the public domain, for the second version we will complete the interviews about the cybercrime investigation best practices as committed to in the task description, specifically focused on the main gaps, needs and areas of focus identified within this deliverable whilst continuing to monitor the public and academic discourse around cybercrime investigation.

For T2.2, as we move towards the definition of the technical specifications the use case scenarios and user requirements will stay under review to ensure alignment between end user needs and the technology being developed. Where new requirements, updates, or changing priorities are identified these will continue to feed into the updated version of this deliverable. Furthermore, with the first planned ENSEMBLE pilots also planned ahead of the next version this deliverable, we will also capture feedback from the piloting phase to update the requirements and user cases to ensure they are practical and implementable within the scope of the project.

9 References

[1] Murphy, C. (2024) Understanding cybercrime. *European Parliamentary Research Service.* Available online: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf

[2] Lusthaus, J. (2024). Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?. *Annual Review of Law and Social Science*, *20*(1), 369-385.

[3] Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic sciences*, *2*(2), 379-398.

[4] Council of Europe (2001) The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols. Available online: https://www.coe.int/en/web/cybercrime/the-budapest-convention

[5] Crown Prosecution Service (2024) CPS Crime Taxonomy. Available at: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

[6] Council of Europe (2012) Cybercrime Convention Committee - Guidance Notes Available online: https://www.coe.int/en/web/cybercrime/guidance-notes

[7] European Commission (n.d.) EU security market study. *Migration and Home Affairs.* Available online: https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study_en

[8] Scroxton, A. (2021). Fraud and cyber crime still vastly under-reported. Computer Weekly, 4. Available online: https://www.computerweekly.com/news/252495844/Fraud-and-cyber-crime-still-vastly-under-reported

[9] CYYBAR Project (2023) Cybercrime against businesses in the EU: Challenges to Reporting. *Policy Brief.* Available online: https://cybbar.eu/cybercrime-against-businesses-in-the-eu-challenges-to-reporting/

[10] Makridis, C., Maschmeyer, L., & Smeets, M. (2024). If it bleeps it leads? Media coverage on cyber conflict and misperception. *Journal of Peace Research*, *61*(1), 72-86.

[11] Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world'policing and law enforcement. *The Police Journal*, *96*(4), 573-592.

[12] Smith, B. (2025) Microsoft launches new European Security Program. *Microsoft.* Available online: https://blogs.microsoft.com/on-the-issues/2025/06/04/microsoft-launches-new-european-security-program/

[13] Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime science*, *7*(1), 1-15.

[14] European Union (2021) MEs and Cybercrime. *Eurobarometer*. https://europa.eu/eurobarometer/surveys/detail/2280

[15] CloudFlare (2024) European businesses anticipate more cybersecurity attacks, but feel unprepared for them. Available online: https://www.cloudflare.com/en-gb/press-releases/2024/european-businesses-anticipate-more-cybersecurity-attacks-but-feel/

[16] European Union (2024) Cyberskills. Europbarometer. Available online: https://europa.eu/eurobarometer/surveys/detail/3176

[17] Porcedda, M. G., & Wall, D. S. (2021). Modelling the cybercrime cascade effect in data crime. In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 161-177). IEEE.

[18] Group-IB (2025) High-tech crime: Trends report 2025. Available online: https://www.group-ib.com/landing/high-tech-crime-trends-2025/

[19] Europol (2025) Internet organised crime threat assessment (IOCTA). European Union Agency for Law Enforcement Cooperation (Europol). Available online: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf

[20] Böhm, I., & Lolagar, S. (2021). Open source intelligence: Introduction, legal, and ethical considerations. *International Cybersecurity Law Review*, *2*(2), 317-337.

[21] ENISA (2024) ENISA Threat landscape. *European Union Agency for Cybersecurity (ENISA).* Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[22] Gobierno de Espana (2023) Informe sobre la cibercriminalidad en España. *Ministerio del Interior.* Available online: https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/en/publicaciones.html

[23] Gobierno de Espana (2025) Portal Estadístico de Criminalidad. *Ministerio del Interior.* Available online: https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/en/

[24] Ministério Público (2024) Dibercrime: denúncias recebidas 2023. *Gabinete Cibercrime* Available online: https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias_cibercrime_2023_2024-09-11.pdf

[25] Ministério Público (2024) Dibercrime: denúncias recebidas 2024. *Gabinete Cibercrime.* Available online: https://cibercrime.ministeriopublico.pt/sites/default/files/2025-03/2025.03.18-denuncias-de-cibercrime-2024.pdf

[26] Council of Europe (n.d.) Romania. *Octopus Cybercrime Community.* Available online: https://www.coe.int/en/web/octopus/-/romania

[27] Ministerul Public (2025) Raport de Activitate 2024. *Direcţia de investigare a infracţiunilor de Criminalitate organizată şi terorism.* Available online: https://www.diicot.ro/images/documents/rapoarte_activitate/raport2024.pdf

[28] Directorate for Investigating Organized Crime and Terrorism. (2025). Number of cybercrimes under the competence of the Directorate for Investigating Organized Crime and Terrorism in Romania from 2010 to 2024 [Graph]. In *Statista*. From https://www.statista.com/statistics/1258159/romania-cyber-crimes-diicot/

[29] Biroul Național de Statistică al Republicii Moldova (2022) Statisticile în domeniul criminalității și justiției din Republica Moldova evaluate în raport cu standardele europene și cele internaționale. Available online: https://statistica.gov.md/ro/statisticile-in-domeniul-criminalitatii-si-justitiei-din-republica-moldova-evalu-12_59733.html

[30] RUSI (2023) Battening Down the Hatches: Moldova's Cyber Defence. *Royal United Services Institute.* Available online: https://www.rusi.org/explore-our-research/publications/commentary/battening-down-hatches-moldovas-cyber-defence

[31] CSIS (2024) Strengthening Moldova's Cyber Landscape. *Centre for Strategi and International Studies .* Available online: https://www.csis.org/analysis/strengthening-moldovas-cyber-landscape

[32] Ministère de L'Intérieur (2024) Rapport annuel sur la cybercriminalité 2024. Available Online: https://www.interieur.gouv.fr/actualites/actualites-du-ministere/rapport-annuel-sur-cybercriminalite-2024

[33] Statista. (2024). Estimated annual cost of cybercrime in France from 2016 to 2028 (in billion U.S. dollars) [Graph]. In Statista, from https://www.statista.com/forecasts/1398948/france-cyber-crime-cost-annual

[34] Ministère de L'Europe et des affaires étrangères (2025) France's international action to fight cyber crime. Available online: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/france-s-international-action-to-fight-cyber-crime-9-jan-2025

[35] UK Government (2024) Cyber security breaches survey 2024. *Department for Science; Home Office.* Available online: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

[36] Statistics Netherlands (2025) More victims of online crime in 2024. Available online: https://www.cbs.nl/en-gb/news/2025/16/more-victims-of-online-crime-in-2024

[37] Federal Ministry Interior, Republic of Austria (2024) Statistics and Graphs. *Criminal Intelligence Service Austria.* Available online: https://www.bundeskriminalamt.at/en/502/start.aspx

[38] Action Fraud (2025) Fraud and cybercrime statistics. Available online: https://www.actionfraud.police.uk/fraud-stats

[39] City of London Police (n.d) NFIB Fraud and Cyber Crime Dashboard. Available online: https://colp.maps.arcgis.com/apps/dashboards/0334150e430449cf8ac917e347897d46

[40] Ministry of Citizen Protection (2025) 24-02-2025: Η ανάρτηση του Υπουργού Προστασίας του Πολίτη Μ. Χρυσοχοΐδη για τον απολογισμό των δράσεων της Δίωξης Ηλεκτρονικού Εγκλήματος. Available online: https://www.minocp.gov.gr/2025/02/24/24-02-2025-i-diefthynsi-dioxis-ilektronikou-egklimatos-einai-apo-tis-ypiresies-aichmis-gia-tin-astynomia-tis-neas-epochis/

[41] Grant Thornton (2021) The economic cost of cybercrime. Available online: https://www.grantthornton.ie/globalassets/1.-member-firms/ireland/insights/publications/grant-thornton---the-economic-cost-of-cybercrime.pdf

[42] Grant Thornton (2022) The cost of cybercrime 2022. Available online: https://www.grantthornton.ie/globalassets/1.-member-firms/ireland/insights/publications/grant-thornton---cost-of-cybercrime-2022.pdf

[43] Tech Central (2025) Third of Irish households have experienced cybercrime. 11 March 2025. Available online: https://www.techcentral.ie/third-of-irish-households-have-experienced-cybercrime/

[44] Lirosi, M. (2025) Cybercrime: 2024 Sets New Record, Italy Among Main Targets. *First Online.* Available online: https://www.firstonline.info/en/cybercrime-il-2024-segna-un-nuovo-record-italia-tra-i-bersagli-principali/

[45] Federal Ministry of the Interior (2025) 2024 National Situation Report on Cyber Crime: Numerous successful investigations, but the threat level remains high. Available online: https://www.bmi.bund.de/SharedDocs/pressemitteilungen/EN/2025/06/pm-lb-cybercrime-en.html

[46] Bundeskriminalamt (2025) Bundeslagebild Cybercrime 2024: BKA setzt anhaltend hoher Cyberbedrohung zahlreiche Ermittlungserfolge entgegen. Available online: https://www.bmi.bund.de/SharedDocs/pressemitteilungen/EN/2025/06/pm-lb-cybercrime-en.html

[47] CREST (2022) Good practice guide: Establishing an effective law enforcement cybercrime unit. *Cyber Security Maturity Assessment Global Ecosystem (CMAGE).* Available online: https://www.crest-approved.org/wp-content/uploads/2022/08/Establishing-an-Effective-Law-Enforcement-Cybercrime-Unit.pdf

[48] Europol (2024) Cybercrime Training Competency Framework. *Europol*. Available online: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Cybercrime%20Training%20Competency%20Framework%202024.pdf

[49] UNODC (n.d.) Global Programme on Cybercrime Training Catalogue. *United Nations Office on Drugs and Crime.* Available online: https://www.unodc.org/unodc/en/cybercrime/training-catalogue

[50] CEPOL (2023) CEPOL OTNA Cyber-attacks. *European Union Agency for Law Enforcement Training.* Available online: https://www.cepol.europa.eu/publications/cepol-otna-cyber-attacks

[51] Council of Europe (2022) Council of Europe HELP online Course on Cybercrime and Electronic Evidence. *Human Rights Education for Legal Professionals.* Available online: https://www.coe.int/en/web/help/-/council-of-europe-help-online-course-on-cybercrime-and-electronic-evidence

[52] College of Policing (2024) Investigation Process. *Authorised Professional Practice.* Available online: https://www.college.police.uk/app/investigation/investigation-process

[53] International Association of Chiefs of Police (2021) Criminal Intelligence. *Law enforcement policy centr.* Available online: https://www.theiacp.org/sites/default/files/2021-08/Criminal%20Intelligence%2008.2021.pdf

[54] College of Policing (2025) Deciding when to use AI. *Authorised Professional Practice.* Available Online: https://www.college.police.uk/guidance/building-ai-enabled-tools-and-systems/deciding-when-use-ai

[55] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

[56] Wright, P., Ysart, N. (2024) Embracing Grading, Handling, and Dissemination Practices in OSINT. *UK OSINT.* Available online: https://www.osint.uk/content/embracing-grading-handling-and-dissemination-practices-in-osint

[57] Vermeulen, G., De Bondt, W., & Van Damme, Y. (2010). *EU cross-border gathering and use of evidence in criminal matters: towards mutual recognition of investigative measures and free movement of evidence?* (Vol. 37). Maklu.

[58] Kusak, M. (2019). Mutual admissibility of evidence and the European investigation order: aspirations lost in reality. In *ERA forum* (Vol. 19, No. 3, pp. 391-400). Berlin/Heidelberg: Springer Berlin Heidelberg.

[59] Ligeti, K., Garamvölgyi, B., Ondrejová, A., & Von Galen, M. G. (2020). Admissibility of Evidence in Criminal Proceedings in the EU. *Eucrim: the European Criminal Law Associations' fórum*, (3), 201-208.

[60] Depauw, S. (2020). In search of a free movement of forensic evidence: Towards minimum standards to determine evidence admissibility?. *Journal of forensic and legal medicine*, *74*, 102021.

[61] ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence https://www.iso.org/standard/44381.html?browse=tc

[62] ISO/IEC 27042:2015 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence https://www.iso.org/standard/44406.html?browse=tc

[63] Quinn, P., Conti, M., Shamah, J. (2021) D7.10 Draft Standards. Lawful evidence collecting and continuity platform development (LOCARD). GA Number: 832735.

[64] Police Scotland (2025) Standard Operating Procedures. Available online: https://www.scotland.police.uk/access-to-information/policies-and-procedures/standard-operating-procedures/

[65] Police Scotland (2018) Crime Investigation – Standard Operating Procedure. Available online: https://www.scotland.police.uk/spa-media/uwwcamlx/crime-investigation-sop.pdf

[66] SO/IEC 27043:2015 Information technology — Security techniques — Incident investigation principles and processeshttps://www.iso.org/standard/44407.html?browse=tc

[67] Clancy, D. (2022). *Development of a Ransomware Investigation Playbook for the Financial Sector, in compliance with ISO/IEC 27043* (Doctoral dissertation, University College Dublin. School of Computer Science).

[68] Council of Europe (2001) The European Code of Police Ethics. *Recommendation CM/Rec(2001)10 and explanatory memorandum.* Available online: https://rm.coe.int/the-european-code-of-police-ethics-pdf/1680b003e0

[69] Council of Europe (n.d.) Training materials, guides, templates. *Octopus Cybercrime Community.* Available online : https://www.coe.int/en/web/octopus/training

[70] SO/IEC 27050-1:2019 Information technology — Electronic discovery Part 1: Overview and conceptshttps://www.iso.org/standard/78647.html

[71] Opinion No.10 (2015) of the Consultative Council of European Prosecutors to the Committee of Ministers of the Council of Europe on the role of prosecutors in criminal investigations https://rm.coe.int/1680747720

[72] Jeffries, S. and Apeh, E. (2020). Standard operating procedures for cybercrime investigations: a systematic literature review. *Emerging cyber threats and cognitive vulnerabilities*, 145-162.

[73] Bandler, J., & Merzon, A. (2020). *Cybercrime investigations: A comprehensive resource for everyone*. CRC Press.

[74] Ciardhuáin, S. Ó. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence*, *3*(1), 1-22.

[75] Hunton, P. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. *Computer Law & Security Review*, *27*(1), 61-67.

[76] Gruber, J., Voigt, L. L., Benenson, Z., & Freiling, F. C. (2022). Foundations of cybercriminalistics: From general process models to case-specific concretisations in cybercrime investigations. *Forensic Science International: Digital Investigation*, *43*, 301438.

[77] Bandler, J., & Merzon, A. (2020). Law Enforcements Cybercrime Investigation. In *Cybercrime Investigations.* CRC Press

[78] UNODC (n.d.) Teaching Model Series Cybercrime: Module 5 Cybercrime Investigation. *Sharing Electronic Resources and Laws on Crime (SHERLOC).* Available online: https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-5/index.html

[79] [79] UNODC (n.d.) Teaching Model Series Cybercrime. *Sharing Electronic Resources and Laws on Crime (SHERLOC).* Available online: https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime.html

[80] Interpol (2021) National Cybercrime Strategy Guidebook. Available online: https://www.interpol.int/content/download/16455/file/Cyber_Strategy_Guidebook.pdf

[81] World Bank (2016) Combatting cybercrime: Tools and capacity building for emerging economies. *Combatting Cybercrime.* Available online: https://www.combattingcybercrime.org/

[82] Cybercrime Programme Office of the Council of Europe (C-PROC) (2019) Standard operating procedures for the collection, analysis and presentation of electronic evidence. *CyberSouth – Cooperation on cybercrime in the Southern Neighbourhood.* Available online: https://rm.coe.int/3692-sop-electronic-evidence/168097d7cb

[83] OSCE (2022) Guidelines on cybercrime investigation. *Organisation for Security and Co-operation in Europe – Presence in Albania.* Available online: https://www.osce.org/files/f/documents/a/8/534684.pdf

[84] Bekkers, L., Leukfeldt, R., & Kleemans, E. (2025). Police Investigations Into Financial-Economic Cybercriminal Networks: The Experiences and Perceptions of Dutch Law Enforcement. *European Journal on Criminal Policy and Research*, 1-20.

[85] Hunton, P. (2011). A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. *Digital investigation*, *7*(3-4), 105-113.

[86] Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal*, *96*(4), 573-592.

[87] De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., ... & Martin, R. (2021). A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists. *Policing: A Journal of Policy and Practice*, *15*(2), 1429-1445.

[88] Steinmetz, K. F., Schaefer, B. P., McCarthy, A. L., Brewer, C. G., & Kurtz, D. L. (2024). Exploring Cybercrime Capabilities: Variations Among Cybercrime Investigative Units. *Criminal Justice Policy Review*, *35*(4), 194-215.

[89] Eurojust (2020) Overview Report – Challenges and best practices from Eurojust's casework in the area of cybercrime. Available online: https://www.eurojust.europa.eu/sites/default/files/assets/2020_11_cybercrime_report.pdf

[90] European Commission (2023) E-evidence - cross-border access to electronic evidence. Available online: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en

[91] Buhrig, R. (2023). Capacity, capability, and collaboration: a qualitative analysis of international cybercrime investigations from the perspective of Canadian investigators. *International Cybersecurity Law Review*, *4*(4), 415-429.

[92] Cibaku, E. (2024). *Cybercrime Investigation in England and Wales: Analysing the Case Failures in Cyber Crime Units* (Doctoral dissertation, University of Portsmouth).

[93] Grochmal, A. B. (2025). *Challenges Faced by Law Enforcement Collecting and Using Digital Evidence in Cybercrime Investigations* (Doctoral dissertation, Marymount University).

[94] Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys (CSUR)*, *54*(11s), 1-37.

[95] Alzahrani, S., Xiao, Y., Asiri, S., Zheng, J., & Li, T. (2025). A Survey of Ransomware Detection Methods. *IEEE Access*.

[96] Baker, K. (2023) How Does Ransomware Spread? 10 Most Common Infection Methods. *Crowdstrike.* Available online: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/how-ransomware-spreads/

[97] Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science*, *8*(1), 1-22.

[98] NCSC (2021) NCSC Annual Review 2021. *National Cyber Security Centre.* Available online: https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threat/ransomware-threat-methodology

[99] Matthijsse, S. R., van 't Hoff-de Goede, M. S., & Leukfeldt, E. R. (2023). Your files have been encrypted: A crime script analysis of ransomware attacks. *Trends in Organized Crime*, 1-27.

[100] Teichmann, F. (2025). Ransomware extortion in Europe: legal responses and mitigation strategies. *International Cybersecurity Law Review*, 1-33.

[101] Adam. S (2024) The role of law enforcement in remediating ransomware attacks. *Sophos.* Available online: https://news.sophos.com/en-us/2024/05/14/the-role-of-law-enforcement-in-remediating-ransomware-attacks/

[102] Magnet Forensics (2021) Anatomy of a Ransomware Investigation. Available online: https://www.magnetforensics.com/blog/anatomy-of-a-ransomware-investigation/

[103] Meurs, T., Hoheisel, R., Junger, M., Abhishta, A., & McCoy, D. (2025). What To Do Against Ransomware? Evaluating Law Enforcement Interventions. In *Symposium on Electronic Crime Research, eCrime 2024*.

[104] Written evidence submitted by RUSI Cyber and the Centre for Financial Crime and Security Studies at RUSI. Available online: https://committees.parliament.uk/writtenevidence/114435/html/

[105] House of Lords, House of Commons (2023) A hostage to fortune: ransomware and national security. *Joint Committee on the National Security Strategy.* Available online: https://committees.parliament.uk/publications/42493/documents/211438/default/

[106] Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., & Chua, Y. T. (2022). Influence, infrastructure, and recentering cybercrime policing: Evaluating emerging approaches to online law enforcement through a market for cybercrime services. *Policing and Society*, *32*(1), 103-124.

[107] Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, *34*, 231-245.

[108] Richet, J. L. (2022). How cybercriminal communities grow and change: An investigation of ad-fraud communities. *Technological Forecasting and Social Change*, *174*, 121282.

[109] Ohm, P. (2017). The investigative dynamics of the use of malware by law enforcement. *Wm. & Mary Bill Rts. J.*, *26*, 303.

[110] Financial Action Task Force (2023) Illicit Financial Flows from Cyber-Enabled Fraud. *FATF, INTERPOL & EGMONT Group.* Available online: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf

[111] Ou, H., Guo, Y., Huang, C., Zhao, Z., Guo, W., Fang, Y., & Huang, C. (2021, December). No pie in the sky: The Digital Currency Fraud Website Detection. In *International Conference on Digital Forensics and Cyber Crime* (pp. 176-193). Cham: Springer International Publishing.

[112] Klom, I. A. (2024). Clusters and Copies: An Analysis of Cryptocurrency Investment Scam Websites. TU Delft. MSc. Thesis.

[113] Ribaux, O., & Souvignet, T. R. (2020). "Hello are you available?" Dealing with online frauds and the role of forensic science. *Forensic Science International: Digital Investigation*, *33*, 300978.

[114] Tidy, J. (2024) Telegram: 'The dark web in your pocket'. *BBC News.* Available online: https://www.bbc.co.uk/news/articles/cdey4prn3e1o

[115] Clarke, S. (n.d.) OSINT: The Key to Dark Web Investigations for Law Enforcement . *Blackdot Solutions.* Available online: https://blackdotsolutions.com/blog/dark-web-law-enforcement/

[116] Goodison, S. E., Woods, D., Barnum, J. D., Jackson, B. A., & Kemerer, A. R. (2019). Identifying law enforcement needs for conducting criminal investigations involving evidence on the dark web. *RAND*. Available online: https://www.rand.org/pubs/research_reports/RR2704.html

[117] DarkOwl (2025) Dark Web Under Watch: Regulation, Enforcement, and the Power of Threat Intelligence Tools. Available online: https://www.darkowl.com/blog-content/dark-web-under-watch-regulation-enforcement-and-the-power-of-threat-intelligence-tools/

[118] Searchlight Cyber (n.d) Case Study – State Government Department in the United States. Available online: https://slcyber.io/wp-content/uploads/2025/05/Case-Study_US-State-Gov-Dept.pdf

[119] Emmen, B., de Poot, C., & Stol, W. (2023). What are they doing in the dark: Police strategies and working methods in fighting crime on the Tor Network. European Journal of Policing Studies, 6(4), 1-21.

https://doi.org/10.5553/EJPS.000003

[120] Interpol, NTU and CFLW Cyber Strategies (2020) Combatting Cyber-enabled Financial Crimes in the era of Virtual Asset and Darknet Service Providers

[121] Department of Justice (2020) Audit of the Federal Bureau of Investigation's Strategy and Efforts to Disrupt Illegal Dark Web Activities. *Office of the Inspector General.* Available online: https://oig.justice.gov/sites/default/files/reports/21-014.pdf

[122] U.S. Department of Justice (2020) Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources. *Cybercrime Unit – Computer crime and intellectual property service criminal division.* Available online: https://www.justice.gov/criminal/criminal-ccips/page/file/1252341/dl?inline

[123] Davies, G. (2020). Shining a light on policing of the dark web: an analysis of UK investigatory powers. *The Journal of Criminal Law*, *84*(5), 407-426.

[124] Jones, M. R. (2020). *Law Enforcement Techniques in Darknet Markets: A Case Study* (Doctoral dissertation, Capitol Technology University).

[125] Rahman, M. D. (2025). The Art of Open Source Intelligence (OSINT): Addressing Cybercrime Opportunities and Challenges. Available at SSRN: https://dx.doi.org/10.2139/ssrn.5281845

[126] Agbu, E. (2024) The Role of OSINT in the Evolution of Threat Intelligence. *UK OSINT Community*. Available online: https://www.osint.uk/content/the-evolution-of-threat-intelligence

[127] Wright, P. (2024) Ethical Dilemma of Using Data Breach Information in OSINT. *LinkedIn.* Available online: https://www.linkedin.com/pulse/ethical-dilemma-using-data-breach-information-osint-paul-wright-jmmaf/

[128] OSCE (2022) Guidelines on Cybercrime Investigation . Organization for Security and Cooperation in Europe. Available online: https://www.osce.org/files/f/documents/a/8/534684.pdf

[129] Cyber Huntress (2024) Conducting OSINT on the Dark Web: Methods and Best Practices. Available online: https://medium.com/@thecyberhuntress/conducting-osint-on-the-dark-web-methods-and-best-practices-da8dc0df6286

[130] VaaData (2024) Cybersecurity OSINT: Methodology, Tools and Techniques. Available online: https://www.vaadata.com/blog/cybersecurity-osint-methodology-tools-and-techniques/

[131] Gupta, K., Oladimeji, D., Varol, C., Rasheed, A., & Shahshidhar, N. (2023). A comprehensive survey on artifact recovery from social media platforms: approaches and future research directions. *Information*, *14*(12), 629.

[132] Quick, D., & Choo, K. K. R. (2018). Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+ OSINT): A timely and cohesive mix. *Future Generation Computer Systems*, *78*, 558-567.

[133] OSINT Industries Team (2025) Scrubbing Up On OSINT Cyber Hygiene (Best Practices). *OSINT Industries.* Available online: https://www.osint.industries/post/scrubbing-up-on-osint-cyber-hygiene-best-practices

[134] Spiekermann, D., & Keller, J. (2024, September). Challenges of Digital Investigations in Nowadays Communication Networks. In 2024 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 872-877). IEEE.

[135] Rizvi, S., Scanlon, M., Mcgibney, J., & Sheppard, J. (2022). Application of artificial intelligence to network forensics: Survey, challenges and future directions. *IEEE Access*, *10*, 110362-110384.

[136] Goel, S., & Nussbaum, B. (2021). Attribution across cyber attack types: network intrusions and information operations. *IEEE Open Journal of the Communications Society*, *2*, 1082-1093.

[137] Europol (2021), Cryptocurrencies - Tracing the evolution of criminal finances,

Europol Spotlight Report series, Publications Office of the European Union, Luxembourg. Available online: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

[138] Home Office UK (2023) Gaps and needs of LEA practitioners in the area of cryptocurrency as a facilitator for cybercrime – public version. *CYCLOPES project.* Available online: https://backend.cyclopes-project.eu/wp-content/uploads/2023/12/Gaps-and-Needs-of-LEA-Practitioners-in-the-Area-of-Cryptocurrency-as-a-Facilitator-for-Cybercrime_.pdf

[139] FTI Consulting (2024) Unravelling the Flow of Funds from a Forensic Perspective. *Lexology.* Available online: https://www.lexology.com/library/detail.aspx?g=3baf837a-ce45-48a4-ae4f-623ee2685b03

[140] Monrow, B. (2024) ACFCS Contributor Report: Bitcoin Tracking for Law Enforcement - A Guide to Crypto Investigations. *Association of Certified Financial Crime Specialists.* Available online: https://www.acfcs.org/acfcs-contributor-report-bitcoin-tracking-for-law-enforcement

[141] Basel Institute for Governance (2023) Quick Guide 1: Cryptocurrencies and money laundering investigations. Available online: https://baselgovernance.org/publications/quick-guide-1-cryptocurrencies-and-money-laundering-investigations

[142] Chainalysis Team (2023) The Chainalysis Law Enforcement Crypto Field Guide. *Chainalysis.* Available online: https://www.chainalysis.com/blog/law-enforcement-crypto-field-guide/

[143] TRM Labs (2024) Tackling Crypto Crime: 2023 Survey of Law Enforcement. Available online: https://www.trmlabs.com/resources/reports/tackling-crypto-crime-2023-survey-of-law-enforcement

[144] Chow, A. R. (2022) 'Crypto Is Anything But Private.' An Author Examines Crime on the Blockchain. *Time.* Available online: https://time.com/6239364/crypto-criminals-andy-greenberg/

[145] Irwin, A. S., & Dawson, C. (2019). Following the cyber money trail: Global challenges when investigating ransomware attacks and how regulation can help. *Journal of money laundering control*, *22*(1), 110-131.

[146] Blockchain Intelligence Group (2025) Digital Detectives – A step-by-step guide for cryptocurrency investigations for law enforcement. Available online: https://blockchaingroup.io/wp-content/uploads/2025/02/Law-Enforcement-Resource-Guide-for-Cryptocurrency-Investigations-.pdf

[147] OSCE (202X) Decoding crypto crime – a guide for law enforcement . Available at : https://www.osce.org/files/f/documents/2/1/587475.pdf

[148] Hancock, P. J., van Hardeveld, G. J., Jakubcek, J., Akhgar, B., Davey, S., & Amann, P. (2024). Design of Cryptopol: A serious game for teaching cryptocurrency tracing techniques to Law Enforcement. *ACM Games: Research and Practice*, *2*(4), 1-14.

[149] Fröwis, M., Gottschalk, T., Haslhofer, B., Rückert, C., & Pesch, P. (2020). Safeguarding the evidential value of forensic cryptocurrency investigations. *Forensic Science International: Digital Investigation*, *33*, 200902.

[150] Woods, D., Hollywood, J. S., Barnum, J. D., Fenimore, D., Vermeer, M. J., & Jackson, B. A. (2023). Cryptocurrency and Blockchain Needs for Law Enforcement. *RAND.* Available online: https://www.rand.org/pubs/research_reports/RRA108-17.html

[151] FTI Consulting (2025) Leveraging Traditional Investigation Data Sources and Methods for a Crypto Investigation. *Lexology.* Available online: https://www.lexology.com/library/detail.aspx?g=af111eda-d6e1-460e-8143-7f41bf0cb6e4

[152] Alghamdi, A. (2025). Forensic Analysis of Cryptocurrency-Based Ransomware Attacks: Criminal Justice and Technical Perspectives. Available at:

https://aziz707.info/research/Forensic_Analysis_of_Cryptocurrency_Based_Ransomware_Attacks__Criminal_Justice_and_Technical_Perspectives.pdf#page=27.80

[153] Council of Europe (2014) Rules on obtaining subscriber information. *Cybercrime convention committee.* Available online: https://rm.coe.int/16802e7ad1

[154] Mir, R., Mackey, A. (2025) How Cops Can Get Your Private Online Data. *Electronic Frontier Foundation.* Available online: https://www.eff.org/deeplinks/2025/06/how-cops-can-get-your-private-online-data

[155] Europol (2024) Sirius Project – Sirius Cross-border access to electronic evidence. Available online: https://www.europol.europa.eu/operations-services-innovation/sirius-project

[156] HLEG on Access to Data for Law Enforcement (2024) Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement. *DG Migration and Home Affairs.* Available online: https://home-affairs.ec.europa.eu/document/download/1105a0ef-535c-44a7-a6d4-a8478fce1d29_en?filename=Recommendations%20of%20the%20HLG%20on%20Access%20to%20Data%20for%20Effective%20Law%20Enforcement_en.pdf

[157] HLEG on Access to Data for Law Enforcement (2024) Concluding report of the High-Level Group on access to data for effective law enforcement. *DG Migration and Home Affairs.* Available online: https://home-affairs.ec.europa.eu/document/download/4802e306-c364-4154-835b-e986a9a49281_en?filename=Concluding%20Report%20of%20the%20HLG%20on%20access%20to%20data%20for%20effective%20law%20enforcement_en.pdf

[158] Council of Europe (2020) Cooperation between law enforcement and Internet service providers against cybercrime: towards common guidelines. *Cybercrime Programme Office of the Council of Europe (C-PROC)*. Available online: https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7

[159] Home Office UK (2023) Gaps and needs of LEA practitioners in the area of investigations involving cloud services – public version. *CYCLOPES project.* Available online: https://backend.cyclopes-project.eu/wp-content/uploads/2023/12/Gaps-and-Needs-of-LEA-Practitioners-in-the-Area-of-Investigations-involving-Cloud-Services_.pdf

[160] COM(2025) 349 final. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Roadmap for lawful and effective access to data for law enforcement. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0349

[161] Hull, M. (2025) How UK Law Enforcement and the Cyber Security Industry Can Collaborate to Combat Cybercrime. *NCC Group.* Available online: https://www.nccgroup.com/uk/how-uk-law-enforcement-and-the-cyber-security-industry-can-collaborate-to-combat-cybercrime/

[162] Europol (2015) EMAS – a solution to analyse binaries. Available online: https://www.europol.europa.eu/sites/default/files/documents/edoc-801456-v2-31__-emas_2.pdf

[163] Europol (2022) Europol Programming Document. Available online: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2023-2025.pdf

[164] Ianelli, N., Kinder, R. Roylo, C. (2007) The Use of Malware Analysis in Support of Law Enforcement. *CERT Coordination Center*. Available online: https://insights.sei.cmu.edu/documents/272/2007_019_001_51051.pdf

[165] FIRST (2024) Malware Analysis Framework Available online: https://www.first.org/global/sigs/malware/ma-framework/

[166] Council of Europe (2023) Guideline for prosecutors and law enforcement in cybercrime investigations in Türkiye. *Strengthening the Criminal Justice System and the Capacity of Justice Professionals on Prevention of European Convention on Human Rights Violations in Türkiye*. Available online: https://rm.coe.int/guide-on-fight-against-cybercrime/1680ae6859

[167] Salvation Data Technology (2024) Key Steps in Malware Analysis for Digital Forensics Investigations. Available online: https://www.salvationdata.com/knowledge/malware-analysis/

[168] Das, S. K, (2024) Malware Analysis in Digital Forensics. *Medium*. Available online: https://medium.com/@sourabhkumardas/malware-analysis-in-digital-forensics-91f401b3f308

[169] Kennedy, I., Bandara, A., & Price, B. (2022). Evaluating Malware Forensics Tools. *arXiv preprint arXiv:2209.12683*.

[170] KPMG (2013) Cyber threat intelligence and the lessons from law enforcement. *KPMG International Cooperative.* Available online: https://assets.kpmg.com/content/dam/kpmg/pdf/2013/02/cyber-threat-intelligence-final3.pdf

[171] Coker, J. (2024) Why Law Enforcement Needs Threat Intelligence from the Cybersecurity Industry. *Infosecurity Europe.* Available online: https://www.infosecurityeurope.com/en-gb/blog/regulation-and-policy/law-enforcement-cybersecurity-threat-intelligence-sharing.html

[172] Cyber Peace Institute and University College Dublin (2024) Cyber threat landscape of EU NGOs and requirements for threat intelligence exchange with Law Enforcement Agencies. UNDERSERVED project. Available online: https://underserved-project.eu/report/UNDERSERVED_REPORT_EN.pdf

[173] UCD CCI (2025) Underserved. Available online: https://github.com/UCD-CCI/Underserved

[174] Lockheed Martin (n.d.) Cyber Kill Chain. Available online: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[175] MITRE (2025) The MITRE ATT&CK Framework. Available online: https://attack.mitre.org/

[176] Sarkar, G., Singh, H., Kumar, S., & Shukla, S. K. (2023). Tactics, techniques and procedures of cybercrime: A methodology and tool for cybercrime investigation process. In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (pp. 1-10).

[177] Alaeifar, P., Pal, S., Jadidi, Z., Hussain, M., & Foo, E. (2024). Current approaches and future directions for cyber threat intelligence sharing: A survey. *Journal of Information Security and Applications*, *83*, 103786.

[178] Allegretta, M., Siracusano, G., Gonzalez, R., & Gramaglia, M. (2023). Are crowd-sourced CTI datasets ready for supporting anti-cybercrime intelligence?. *Computer Networks*, *234*, 109920.

[179] MISP (n.d.) MISP features and functionalities. Available online: https://www.misp-project.org/features/

[180] CIRCL.LU (2024) MISP User Stories. *Computer Incident Response Centre Luxembourg.* Available online: https://www.circl.lu/doc/misp/user-stories/

[181] ENSIA (2020) Roadmap on the cooperation between CSIRTS and LE. *Ueopean Union Agency for Cybersecurity.* Available online: https://op.europa.eu/en/publication-detail/-/publication/146d48f1-3387-11eb-b27b-01aa75ed71a1/language-en

[182] NVISO Labs (2022) Visualizing MISP Threat Intelligence in Power BI – An NVISO TI Tutorial. Available online: https://blog.nviso.eu/2022/11/09/visualizing-misp-threat-intelligence-in-power-bi-an-nviso-ti-tutorial/

[183] Chung, M. H. M., Yang, Y. A., Wang, L., Cento, G., Jerath, K., Taank, P., ... & Chignell, M. H. (2023). Enhancing cybersecurity situation awareness through visualization: A USB data exfiltration case study. *Heliyon*, *9*(1).

[184] Jacobson, M., Perbix, M, Lissy, K. (2023) Designing an effective law enforcement data dashboard. U.S. Department of Justice. *Community Oriented Policing Services.* Available online: https://portal.cops.usdoj.gov/resourcecenter/content.ashx/cops-w1012-pub.pdf

[185] Hales, G. A., Ferguson, R. I., & Archibald, J. M. (2012). On the use of data visualization techniques to support digital forensic analysis: A survey of current approaches. *In 2nd International Conference on Cybercrime, Security and Digital Forensics (Cyberforensics 2012).*

[186] Hales, G., & Bayne, E. (2019, June). Investigating visualisation techniques for rapid triage of digital forensic evidence. *In International Conference on Human-Computer Interaction* (pp. 277-293). Cham: Springer International Publishing.

[187] Zákopčanová, K., Řeháček, M., Batrna, J., Plakinger, D., Stoppel, S., & Kozlíková, B. (2020). Visilant: Visual support for the exploration and analytical process tracking in criminal investigations. *IEEE Transactions on Visualization and Computer Graphics*, *27*(2), 881-890.

[188] Carvalho, R. (2018). *Enhancing the investigation of malware-related crimes using semantic technologies* (Doctoral dissertation, University of Oxford).

[189] Genderen, K. V. (2023). *A User-Centered Explainable AI Visualization Study for Enhancing Decision Making in Law Enforcement* (Master's thesis).

[190] Europol (2024) AI and Policing. *Europol Innovation Lab.* Available online: https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing

[191] Jarrett, A., & Choo, K. K. R. (2021). The impact of automation and artificial intelligence on digital forensics. *Wiley Interdisciplinary Reviews: Forensic Science*, *3*(6), e1418.

[192] Ayobami, U. Automated Metadata Extraction and Correlation Techniques for Digital Evidence Analysis in Cybercrime Investigations. Available online: https://ijarpr.com/uploads/V2ISSUE6/IJARPR0605.pdf

[193] Kim, K. J., Lee, C. H., Bae, S. E., Choi, J. H., & Kang, W. (2025). Digital forensics in law enforcement: A case study of llm-driven evidence analysis. *Forensic Science International: Digital Investigation*, *54*, 301939.

[194] Sikos, L. F. (2021). AI in digital forensics: Ontology engineering for cybercrime investigations. *Wiley Interdisciplinary Reviews: Forensic Science*, *3*(3), e1394.

[195] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97, 101804.

[196] Horsman, G. (2024). Commentary:-Can I use that tool?. *Forensic Science International: Digital Investigation*, *51*, 301843.

[197] Horsman, G. (2025). GAMEPLANS: A template for robust digital evidence strategy development. *Journal of Forensic Sciences*, *70*(1), 369-375.

[198] Antwi-Boasiako, A., & Venter, H. (2017). A model for digital evidence admissibility assessment. In *IFIP International Conference on Digital Forensics* (pp. 23-38). Cham: Springer International Publishing.

[199] Steinmetz, K. F., Schaefer, B. P., Brewer, C. G., & Kurtz, D. L. (2025). The role of computer technologies in structuring evidence gathering in cybercrime investigations: A qualitative analysis. *Criminal Justice Review*, *50*(1), 67-84.

[200] Reedy, P. (2023). Interpol review of digital evidence for 2019–2022. *Forensic Science International: Synergy*, *6*, 100313.