D4.1 Network Methods and Tools

Lead Beneficiary	VICOMTECH
Dissemination Level	PUBLIC
Date	29/02/2024
Grant Agreement Number	101121152

Funded by
the European Union

Project Information

Grant Agreement Number	101121152
Acronym	ENACT
Name	European Network Against Crime and Terrorism
Call Topic	HORIZON-CL3-2022-SSRI-01-02 Knowledge Networks for Security Research & Innovation
Action Type	Coordination and Support Action
Start Date	01/09/2023
Duration	36 Months
Coordinator	PJ

Document Information

Work Package	WP4: Network implementation set-up
Deliverable	D4.1 Network methods and tools
Date	29/02/2024
Type	[REPORT]
Dissemination Level	[PUBLIC]
Lead Beneficiary	VICOMTECH
Main Author(s)	VICOMTECH, NP
Contributors	ENG; EOS; FRMDLI; PJ
Document Reviewers	Dorothea Tsatsou (CERTH); André Alegria, Filipe Rodrigues (PJ)
Security Reviewer	Jarmo Puustinen (FIMOI); Rocío Carbayo (ESMIR)
Ethics Reviewer	Isabela Maria Rosal (KUL)

Revision History

Version	Date	Author	Comments
0.1	10/01/2024	VICOM	First draft , Sections 1, 2
0.2	12/02/2024	VICOM	Second draft, Sections 1, 2
0.3	15/02/2024	VICOM	Third draft, Sections 1, 2 and Appendixes A, B and C
0.4	19/02/2024	NP	Fourth draft, adds Section 3
0.5	20/02/2024	VICOM	Final draft
0.6	21/02/2024	PJ	Review
0.7	26/02/2024	CERTH	Review
0.8	27/02/2024	NP	Reviews processed
0.9	27/02/2024	KUL	Ethics Review: check for accessibility, non-discriminatory language use, and transparency; review any mention to ethical or legal issues.
1.0	29/02/2024	FIMOI	Security Review: verify that no security-sensitive information is included in the document, ensure appropriate classification of the deliverable, and confirm that no security-relevant issues are present
1.1	1/03/2024	VICOM	Final
2.0	14/08/2025	VICOM	Updated in line with feedback from EAB and REA expert review.

Disclaimer

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 European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Copyright

Abbreviations

AI	Artificial Intelligence
CapO	Capability Observatory
CDE	Communication Dissemination and Exploitation
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CERIF	Common European Research Information Format
CERIS	Community of European Research and Innovation for Security
CL3	Cluster 3
CM	Capability Map
COTS	Commercial Off-the-Shelve
CPV	Common Procurement Vocabulary
C-UAS	Counter Unmanned Aerial Systems
DCE	Dissemination Communication and Exploitation
DTW	Detailed Task Workplan
EACTDA	European Anti-Cybercrime Technology Development Association
EARTO	European Association of Research and Technology Organisations
ECSO	European Cyber Security Organisation
ELSO	Ethical, Legal & Societal Observatory
EM	Ethical, Legal & Societal Map
EMPACT	European Multidisciplinary Platform Against Criminal Threats
ENFSI	European Network of Forensic Science Institutes
ENLETS	European Network of Law Enforcement Technology Services
EPCC	European Police Chiefs Convention
ETSI	European Telecommunications Standards Institute
EU	European Union
EUCB	EU Clearing Board
EUCI	EU Classified Information
FCT	Fight against Crime and Terrorism
FDO	Fair Data Objects
FKR	Flash Knowledge Report
FP	Framework Programme
H2020	Horizon 2020
INTERPOL	International Criminal Police Organization
IOC	Inter Observatory Coordinator
ISO	International Standardisation Organisation
KER	Key Exploitable Results
KH	Knowledge Hub
KO	Knowledge Observatory

KPI	Key Performance Indicator
KR	Knowledge Repository
L1	Level 1
L2	Level 2
L3	Level 3
LEA	Law Enforcement Agency
MFSO	Market, Funding & Standardisation Observatory
MM	Market Map
MS	Member State
PUB	Public
R&D&I	Research and Development and Innovation
R&I	Research and Innovation
RSS	Really Simple Syndication
RTO	Research and Technology Organisation
SEN	Sensitive
SKB	Knowledge Base
SoP	State of Play
SSRI	Strengthened Security Research and Innovation
TBD	To be defined
TechO	Technology Observatory
TM	Technology Map
TRL	Technology Readiness Level
TX.1/2/3/4	Tasks 1, 2, 3 and 4 of Work Packages 5, 6 and 7
URL	Uniform Resource Locator
WP	Work Package

List of Figures

List of Tables

Table of Contents

Executive Summary

This deliverable presents the RESEARCH tools and the NETWORKING tools set-up by the ENACT project which will be further developed during the implementation cycles. The work of this deliverable has been carried out under the tasks T4.1 and T4.2.

The ENACT RESEARCH pillar will set-up an Observatory system that will count with a Capability Observatory, a Technology Observatory, a Market, funding & Standardisation Observatory and an Ethical, Legal & Societal Observatory. In addition to these four knowledge areas, a fifth observatory, the so-called Inter-Observatory Coordinator (IOC), will merge the knowledge delivered by the others and deliver it in a common FCT R&I knowledge picture.

Each of the observatories has been defined to set the boundaries of their respective fields of interest. These fields of interest include, among others, fight against crime and terrorism (FCT) policy priorities, security threats and security functions (CapO), main science and technology trends, R&I outcomes and Commercial Off-the-shelve (COTS) products (TechO), tender opportunities, industrial fairs and exhibitions and standardisation (MFS), and ethical, legal and societal aspects to guarantee the development of initiatives and creation of knowledge ethically and legally based (ELSO). The leadership, contributors and functioning of the observatories have also been defined, establishing a process of planning, operation and reporting that will be executed during each implementation cycle foreseen in the project. During such implementation cycles, the observatories will produce various ENACT products, including the FCT Maps, Flash reports, Advanced Analytical Reports and Annual State of Play FCT Policy Reports. The scope and main aspects to be considered in the elaboration of these products have been defined in this strategy in order to facilitate their release, notably during the test implementation cycle. Among the main tools to be used by the observatories to carry out their work, the following have been included: The EU Security taxonomy, the ENACT Structured Knowledge Base (SKB), and a set of online data acquisition tools. The latest will be mainly used to retrieve information from the main data sources identified in this strategy as a starting point.

The ENACT NETWORKING pillar will display the tools needed to articulate the network, namely the ENACT Stakeholder Map, the Stakeholder register and the ENACT NETWORKING Logfile.

The Stakeholder map visualizes all ENACT communities of interest and the 3 main target groups of stakeholders (Knowledge Hubs, relevant organisations and experts). In the Stakeholder register, all stakeholders will be registered including the Point of Contact (PoC) from the ENACT consortium and from the Stakeholder organisation. Finally the ENACT NETWORKING logfile will log all registered interactions, connections and related communications and exchanged knowledge so that the project can monitor the progress and the compliance to the KPIs for the NETWORKING pillar. During the upcoming 3 implementation cycles the Stakeholder map, the tools and the (internal) procedures and responsibilities will be monitored, evaluated and updated if needed.

1 Introduction

1.1 ENACT Concept and Approach

Knowledge is one of the most strategic assets available to the European Union. The ability to anticipate threats, adapt to emerging challenges, and ensure evidence-based policymaking depends not only on technological capabilities or operational readiness, but also on the existence of robust, structured, and accessible knowledge ecosystems. Recognising this, the European Commission, through DG HOME, launched a dedicated effort to establish Knowledge Networks in key security domains, including the fight against crime and terrorism, border management, disaster resilience, among others.

The creation of these networks responds to a fundamental challenge: while Europe has invested heavily in security research and operational innovation, the results of these efforts are often fragmented, difficult to access, or disconnected from the needs of practitioners. Valuable knowledge produced in EU-funded projects, national initiatives, or institutional bodies frequently remains isolated within specific communities, limiting its practical impact and slowing the uptake of innovation.

Knowledge Networks are intended to address this structural gap. By promoting cooperation, knowledge sharing, and strategic alignment among researchers, practitioners, policymakers, and industry, these initiatives seek to create long-term, service-oriented platforms that consolidate existing expertise and make it actionable. More than just repositories or research summaries, these networks are designed to foster dialogue, support policy development, and contribute to the long term resilience and effectiveness of the security of the European Union.

Through these efforts, DG HOME aims to ensure that the wealth of knowledge already produced, and still to come, can be better organised, better used, and ultimately better connected to the priorities of the Union and its citizens.

ENACT – European Network Against Crime and Terrorism – is one of the thematic Knowledge Networks aiming to strengthen Europe's capacity to fight crime and terrorism through structured knowledge, strategic collaboration, and innovation uptake. As a network, ENACT brings together law enforcement agencies, researchers, policymakers, and industry to collect, organise, and make sense of the vast and fragmented body of knowledge generated across the FCT landscape. It provides a platform for sharing insights, identifying gaps, validating solutions, and aligning research and innovation with real operational needs, serving as both a knowledge hub and a bridge between research and practice.

1.2 Purpose of this Deliverable and links with other Deliverables

Following the indications of the Commission for the operation of practitioner/knowledge networks, ENACT builds upon 4 overarching pillars, namely Networking, Research,

Communication, Dissemination and Exploration (CDE), and Cooperation[1]. Each of this pillars has been addressed by the WP4 tasks T4.1, T4.2, T4.3 and T4.4.

This Deliverable D4.1 aims to present the high-level strategy to build and operationalise two key pillars of the ENACT architecture, namely the Research pillar and the Networking pillar. The deliverable introduces the methods and procedures to be followed during the project implementation stages in order to collect, exploit and share knowledge within the FCT community.

The RESEARCH pillar is pivotal to project activities, focusing on generating actionable feedback for the EU FCT R&I Community. ENACT will implement an observatory system to extract, classify, and visualize information from the community through Knowledge Hubs, ultimately providing valuable feedback to stakeholders..

The Commission and the Agencies have fostered the creation of an ecosystem of cooperation between the different actors in the EU Security R&I domain that facilitates the interaction among them and aims to facilitate the flow of information. However, the dynamics of this ecosystem are extremely complex, as shown by previous attempts to depict it (e.g. as in the EU security Market Study[2] or in projects such as MEDEA9 [3]). ENACT will build on a strong NETWORKING pillar, identifying the role of each actor in the Security R&I ecosystem and interacting with them according to their mandates and objectives. To that aim, the project will not aspire to connect with every single stakeholder and absorb as many as possible under its direct constituency (efforts that proved futile in previous networks), rather it will propose a strategy that connects the project with the main Knowledge Hubs of the FCT ecosystem. Through these hubs, ENACT will find a way to better structure, format and channel the knowledge needed and generated by the project from and to the main communities of interest, including policymakers, LEAs, industry, RTOs and civil society.

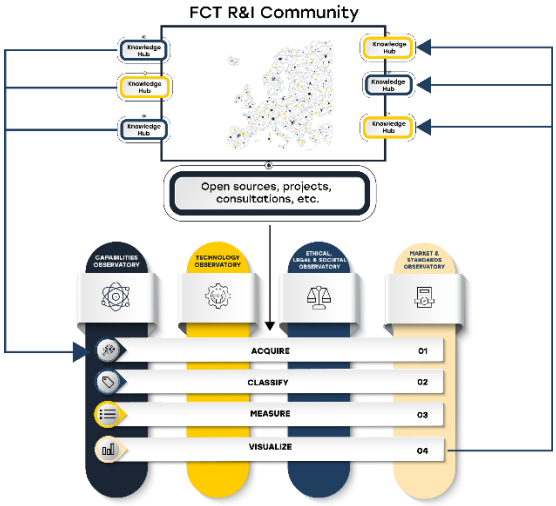


Figure 1 – Conceptual view of ENACT's research and networking pillars

[1] "Interacting with Networks of Practitioners", European Commission (DG HOME), SEREN4 Project Workshop, 28/04/2020. https://prod5.assets-cdn.io/event/4835/assets/8410617916-e5dc31f16f.pdf

[2] European Commission. EU civil security stakeholder catalogue. Available at: https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study/eu-civil-security-stakeholder-catalogue_en

[3] MEDEA. Stakeholders' map. Retrieved at: https://www.medea-project.eu/interactive-map/

1.3 Intended audience

This deliverable is directed towards the ENACT consortium partners, and in particular to Work Package Leaders of WP 5, 6 and 7, as it will serve as a tool to carry out the tasks to be accomplished during the three implementation cycles.

2 ENACT Research Tools

The RESEARCH pillar is at the core of the project activities, as it aims to generate actionable and evidence-based feedback for the EU FCT R&I Community. In order to do so, ENACT will implement an observatory system that will allow: i) to extract information from the wider FCT R&I Community making use of the project's connections with specific Knowledge Hubs (KH); ii) to classify the information according to a recognisable taxonomy; iii) to define concrete metrics and derive results based on the exploitation of the acquired information; iv) to visualise those metrics in a way that can be easily digested by the information consumers; v) to feed it back to the community, again through the main Knowledge Hubs.

The observatory system will count with four main Knowledge Observatories (KO), which will cover the following domains of interest: i) Capabilities; ii) Technology; iii) Market, funding & standardisation; iv) Ethical, Legal & Societal. In addition to these four knowledge areas, a fifth observatory, the so-called Inter-Observatory Coordinator, will merge the knowledge delivered by the others and deliver it in a common FCT R&I knowledge picture.

The outcomes of the observatory process will be compiled in the Key Exploitable Results (KER) 2 to 5, which will eventually feed into the project deliverables.

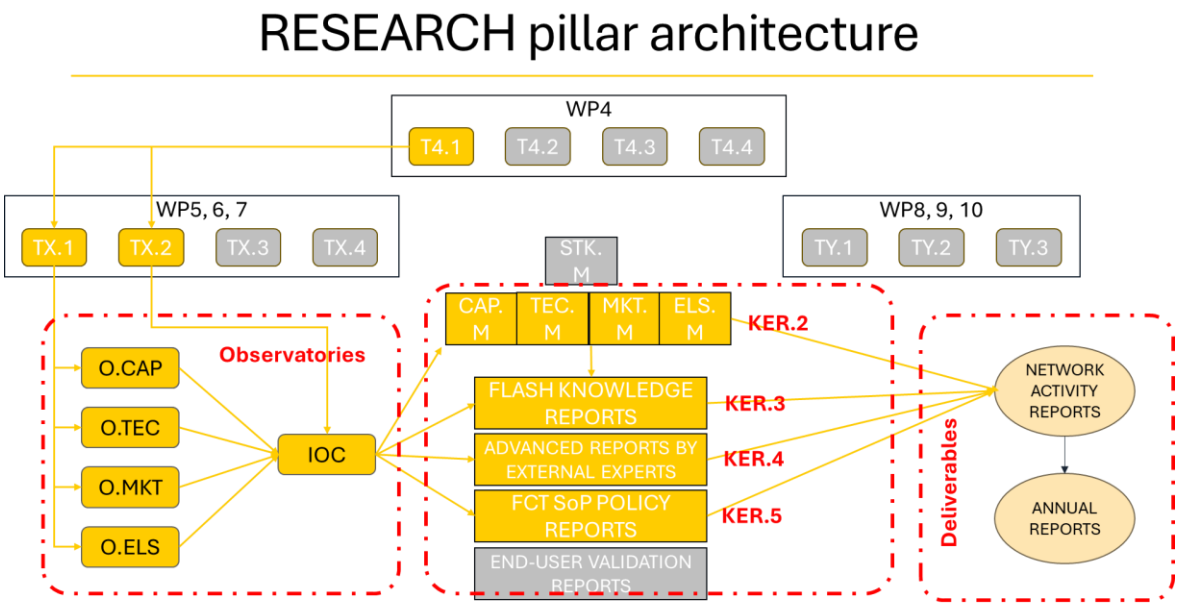


Figure 2 – ENACT's RESEARCH pillar architecture

The operation of the observatories will be based on the conceptual cycle "Acquire / Classify / Measure / Visualise".:

- **Acquire:** The observatories will ingest information from heterogeneous sources, ensuring a broad and permanent surveillance on historic data but also on main trends. The sources to be considered by each observatory may vary in function of the specificities of each knowledge area.
- **Classify:** The information acquired by the observatories will be classified according to different criteria, including the EU Security Market Study taxonomy for the area of FCT. By structuring all the information in the same manner ENACT will create a more homogeneous body of knowledge that can be shared and compared.
- **Measure:** The information acquired and classified in ENACT's Knowledge Repository will be exploited in order to derive concrete intelligence artifacts that shed light on FCT R&I knowledge that is hiding at plain sight. These artifacts will constitute important evidence to support decisions made for the programming of investments in the area of security for policy stakeholders, end-users, procurers, technology suppliers and developers. The observatories will try to define these artifacts in order to allow ready-made results that can be provided upon requests coming at short notice, thus allowing the development of a "knowledge-as-a-service" concept that can provide insights in real time, in addition to the periodic assessments to be elaborated by each observatory in their 6 months reports.
- **Visualise:** It is of utmost importance that the knowledge delivered by the observatories has the right format so that it is easily digestible by the knowledge consumers. The formatting of the reports and the visualisation of the artifacts derived from the exploitation of the information will be handled with care so there is no loss of information and the insights provided have maximum value and clarity.

2.1 Observatory description

2.1.1 Definition

This section proposes a definition for the 4+1 observatories of ENACT. The definition of the knowledge observatories shall serve to set the boundaries of the fields of interest to be addressed by each observatory.

2.1.2 Capability Observatory

As defined in the Work Programme Horizon Europe Cluster 3 2021-2022, the term "Capability" should be understood as "the ability to pursue a particular policy priority or achieve a desired operational effect". The term "capability" is often interchanged with the term "capacity", but this should be avoided. "Capacity" could refer to an amount or volume of which one organisation could have enough or not. On the other hand, "capability" refers to an ability, an aptitude or a process that can be developed or improved in consonance with the ultimate objective of the organisation.

The Capability observatory will consist of a series of resources deployed and operated by a multidisciplinary team of ENACT partners dedicated to strengthening and systematising the vigilance on **FCT policy priorities, security threats and security functions** required to achieve the effects desired by EU security authorities and practitioners. Security functions are defined in the Security Market Study 2015 and 2021 as a set of disciplines, activities or processes that enable LEAs operations.

To do so, the observatory will acquire and classify data and information related to the subject matter of interest with the aim to build a dynamic and updated picture of the **main highlights and trends in FCT threats, policy and functions as perceived by the stakeholders, with special attention to the views of the LEAs and security practitioners**. This picture will be reflected in the products to be delivered by the observatory and explained in sections below.

2.1.3 Technology Observatory

ENACT will look at technology with different time perspectives. On one hand, the technology observatory will provide a vision of the products and services currently used by EU LEAs, but also of others already available in the market with an aim of improving the operational effectiveness and efficiency of LEAs. Considering the constantly evolving security landscape as well as the developments in the science and technology domains, the Technology observatory will also ensure a view of the mid and long-term perspectives by ensuring the vigilance of recently finished, ongoing and upcoming FCT R&I projects, and of the latest scientific progress that shall enable the solutions of tomorrow. In both cases, the observatory will be particularly sensitive to technology developed in the EU, as this information will be relevant to raise awareness on the level of technological sovereignty and autonomy of the EU in this particular domain.

Therefore, the observatory will acquire and classify data and information related to the subject matter of interest with the aim of building a dynamic and updated picture of the **main science and technology trends as they emerge from the market and ongoing research.** This picture will rely largely on information provided by LEAs about the current **systems in use, being these from EU or third-country suppliers**, from the **portfolios of the EU Technology and Industrial Base, considering technology offered in the security domain and possibly also in other domains but with potential security application**s, from the main **security technology Research and Development and Innovation (R&D&I) funding programmes at EU and Member State (MS) level** and their participants, and from salient, current R&D&I advances pertaining to the security technology sector within the EU and beyond, as per the expertise of consortium partners over advances of the state of the art**.** The latest will include technologies at both ends of the Technology Readiness Level (TRL) scale, which at more mature stages can be already tailored to FCT domain-specific requirements, but which at lower TRLs are still domain-agnostic but may show potential for addressing FCT challenges. This picture will be reflected in the products to be delivered by the observatory and explained in the sections below.

2.1.4 Market, funding and Standardisation Observatory

The fragmentation of the security market makes it extremely complex to have a timely updated picture of the opportunities to bring technology from early maturity to an operational product stage. ENACT will monitor these opportunities, notably those who come in the form of **grants from EU programmes** as well as **public procurement carried out at EU and MS level**. Regarding EU programmes, the upcoming calls of the **EU-funded security R&I** work programme in the FCT destination will be monitored, but also opportunities coming from non-R&I programmes will be under the spotlight, notably the **Internal Security Fund** and the **EU Anti-Fraud Programme** (others might be added during the implementation cycles). On the

procurement side, **tender procedures** launched at EU and national level will be monitored, notably those under the following Common Procurement Vocabulary (CPV)[4] codes:

- 35000000 - Security, fire-fighting, police and defence equipment
- 45216000 - Construction work for buildings relating to law and order or emergency services and for military buildings
- 50600000 - Repair and maintenance services of security and defence materials
- 73400000 - Research and Development services on security and defence materials
- 73000000 - Research and Development services and related consultancy services
- 80600000 - Training services in defence and security materials

Innovation Procurement initiatives will be monitored closely as per being a significant catalyst for uptake.

The monitoring of fairs and exhibitions relevant to FCT technology held in the EU Member States will also be part of the observatory activities, as they provide a window to understanding the demand and the offer existing in the current market and facilitates business creation.

Emerging challenges in security, such as the aforementioned market fragmentation, pose standardisation efforts to achieve a cohesive and harmonised security framework and thus foster innovation uptake. ENACT will support security practitioners in staying ahead of evolving threats by providing an up-to-date and comprehensive understanding of the latest standards, protocols, and best practices. ENACT partners will be vigilant on a variety of specific standards, dealing with specific issues following the needs expressed by both the industry sector or the operators (e.g. on data protection and security, security evaluation, identity management, etc.) as well as standards used at Members State level (for their own procurement procedures). Different aspects of business operations will be covered including processes, products, communication, and information exchange.

ENACT will also closely monitor the initiatives and progress undertaken by standardisation organisations such as International Organization for Standardization (ISO), European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC) or the European Telecommunications Standards Institute (ETSI). It will also monitor pre-normative initiatives fostered by associations such as the European Cyber Security Organization (ECSO) and the European Network of Law Enforcement Technology Services (ENLETS).

2.1.5 Ethical, Legal and Societal Observatory

R&I in the FCT field must always consider ethical, legal and societal aspects to guarantee the development of initiatives and creation of knowledge ethically and legally based, with increase trustworthiness from society in the law enforcement field.

Understanding this, European Funded research activities should always consider these aspects during their construction, guaranteeing higher levels of excellence with ethical compliant research results. On this, especially in the FCT, knowledge should consider the legal constraints and limitations established, since it is a largely regulated sector, with various

[4] European Commission. **Common procurement vocabulary**. Available at: https://single-market-economy.ec.europa.eu/single-market/public-procurement/digital-procurement/common-procurement-vocabulary_en

risks to the fundamental rights and freedoms. Only with this in mind, it is possible to bring the theorical solutions and findings into concrete implementation. Finally, societal acceptance of the new FCT technologies and approaches are essential to guarantee a better implementation of said novelties. For this aim, it is essential to effectively consider societal opinions during the knowledge development, meaning that, since the initial research steps, engagement activities with different representatives of society should be put into action, for a continuous transparent dialogue between stakeholders.

ENACT Ethical, Legal and Societal Observatory intends to map and explore the different solutions already developed in the FCT field for guaranteeing the implementation of these aspects in the FCT knowledge. For this, the observatory will analyse solutions developed in finished EU funded projects mapped in the other Observatories involving the development of knowledge and new technologies for improving FCT. The observatory will also follow EU funded projects being developed and new calls.

Evaluation will consider actions implemented since the initial research phase (e.g., ethical self-assessment), until continuous processes (e.g., implementation of independent Ethics Advisory Boards, societal engagement activities). Since various results are confidential to the project members, the Observatory will consider the public documents for creating a database for ENACT (e.g., Cordis entries, website publications). Also, considering the constructed network with various law enforcement agencies, it will be possible to better understand and organize already existing efforts taken by these bodies for the implementation and maintenance of legal, ethical and societal approach into FCT activities. Finally, research results will also be considered for completing the findings, with desk-based research. The results of the Observatory should be able to provide insightful inputs for both research activities as well as daily activities of FCT stakeholders, especially when combined with the results found in the other observatories.

However, it is important to clarify that the ELSO does not intend to provide ethical or legal evaluations of any of the observations added to ENACT's knowledge hubs and observatories. The ELSO aims to observe and catalogue the main trends involving ethical, societal and legal aspects in the FCT Community, without further evaluating their initiatives, mitigation measures, or compliance and readiness levels. Future iterations of ENACT's results may count with more specific considerations about ethical, legal and societal aspects, but the focus will solely be on highlighting these aspects, facilitating eventual future assessments and allowing for further exploration of the displayed knowledge.

2.1.6 Inter-Observatory Coordinator

The role of the Inter-Observatory Coordinator will be crucial to guarantee the coordinated action of the four Knowledge Observatories and the production of high quality information products, notably those mentioned in section 3.

The IOC will run under Tasks TX.2[5], therefore, the ENACT partner leading the IOC in each implementation cycle will be the respective partner acting as Task TX.2 leader and also as Work Package Leader in work packages 5, 6 and 7). Therefore, at each implementation cycle

[5] From now on, the terminology TX.Y will be used to refer to tasks carried out during the three implementation cycles, therefore “X” will replace, indistinctively numbers 5, 6 and 7, while “Y” will be used to refer to one of the four tasks that repeat in the three work packages.

it shall be avoided that the corresponding WP leader and IOC also leads any of the four Knowledge Observatories.

At the beginning of each implementation cycle, the IOC will coordinate the definition of the planning of the Observatory activities for the corresponding cycle. In his coordinating role, the IOC will also supervise the planning proposed by each of the other four Observatory leaders and ensure that there is no overlapping or mismatch among them.

The IOC will ensure internal coordination regarding the interaction of ENACT with the external Knowledge Hubs with the Observatory System. This internal coordination will also involve the KO Leaders and the ENACT partners leading Tasks TX.3 and TX.4 in WPs 5, 6 and 7 (liaison with LEAs and liaison with Industry, respectively).

The IOC will be the partner responsible for the production of the products associated to KERs 2, 3, 4 and 5. To do so, the IOC will coordinate contributions from the partners to the different KERs, based on the role of each partner and the contents to be added in the products. Regarding KERs 2 and 4, the main contribution to the products shall be produced by the Observatory Leaders (Capability Maps) and by the External Experts (Advanced Reports by External Experts).

2.2 Leadership and contributions

In each implementation cycle (WP5, WP6 and WP7), the IOC (which is also the WP leader and TX.2 leader) will monitor the implementation of the observatory system, while other project partners will be leading each observatory as a subtask of TX.1.

The appointment of the Observatory Leaders takes into consideration the type of partner, its area of expertise and its correlation with the scope of the observatory. It also avoids that partners responsible for the IOC act also as KO leaders in one same implementation cycle. The following leadership distribution is proposed for the different implementation cycles.

Table 1 – Observatory and Task leadership distribution

	TIC (WP5)	IC1 (WP6)	IC2 Lead (WP7)
WP Leader	**INOV**	**ENG**	**CERTH**
T4.1 Leader	**INOV**	**ENG**	**CERTH**
Cap. Obs	PJ	FIMOI	FRMDLI
Tech. Obs	CENTRIC	CERTH	ENG
Mkt. Obs	EOS	EOS	EOS
ELS Obs	KUL	KUL	KUL
T4.2 Leader	**INOV**	**ENG**	**CERTH**
IOC Leader	INOV	ENG	CERTH
T4.3 Leader	**PJ**	**FIMOI**	**FRMDLI**
T4.4 Leader	**CENTRIC**	**CERTH**	**ENG**

As shown in the table, the leadership of the Capability Observatory (CapO) has been assigned to Law Enforcement Authority (LEA) partners, while the leadership of the Technology Observatory (TechO) has been assigned to RTO/Industry partners. Regarding the Market, Funding & Standardisation Observatory (MFSO) and the Ethical, Legal & Societal Observatory (ELSO), the unique profiles of EOS and KUL respectively make them the best candidates to lead the observatories in the three implementation cycles.

Among other tasks, it will be the responsibility of the Observatory Leaders to:

1. Design and maintain the Observatory acquisition plan;
2. Ensure the involvement of contributing partners and define their observation profiles;
3. Moderate contributions to Knowledge Base, ensuring the quality and relevance of the data acquired;
4. Avoid redundancies and duplications in data acquired;
5. Detect unbalances in acquired data and additional data needs;
6. Produce or manage the production of statistics of acquired data;
7. Updating and maintaining the list of information sources;
8. Lead the planning of the interaction between the Knowledge Observatories and the Knowledge Hubs at the beginning of each cycle, and accompany the Knowledge Observatory leaders in their interaction with the Knowledge Hubs, ensuring that mutual information needs areas are duly addressed.
9. Establish a feedback loop with end-users, contributors, and stakeholders to gather insights on data usability and areas for improvement;
10. Request and provide data to the external Knowledge Hubs and Stakeholders through the Inter-Observatory Coordinator;
11. Draft the corresponding Observatory Map following agreed template, every 6 months and send it to the Inter-Observatory Coordinator for its finalisation and publication.

All the partners with dedication in the Implementation Cycle Work Packages (WP5, WP6, WP7) will make timely contributions to the Knowledge Repository as part of the Observatory activities. Each contributor will contribute **with no less than 10 observations per month to the work of the Observatories**, following the acquisition plan agreed with the Observatory Leader at the beginning of the implementation cycle and reflected in the Detailed Task Workplan (see section 2.5). The contributors will ensure that the data acquired is pertinent to the focus of the observatory and will support in its classification according to the vocabulary structure and metadata defined for the ENACT Structured Knowledge Base (see Section 2.6). The contributors shall propose additional information sources to the Observatory leader during the implementation cycles so the data sources list (see Section 2.8) is timely updated. The contributors will support the Observatory Leaders in the production of the ENACT products and will participate in the elaboration of such products according to the assignments agreed with the Observatory Leaders.

2.3 Stakeholders

Relevant stakeholders for each observatory will be identified in the Networking Strategy (T4.2) and added to the stakeholders Map (KER1). These should be considered both as a source of data/information for the activities of the Observatories and as the consumers of the products delivered.

Considering previous efforts and futile results in previous networks, ENACT will not aspire to connect directly with every single stakeholder and absorb as many as possible under its direct constituency. On the contrary, ENACT proposes a strategy that connects the project with the main **Knowledge Hubs** of the FCT ecosystem. Through these hubs, ENACT will find a way to better structure, format and channel the knowledge needed and generated by the project from and to the main communities of interest, including policy-makers, LEAs, industry, RTOs and civil society.

The main Knowledge Hubs for each community of interest, as identified in the ENACT proposal, and their relevance as a source of information to the different observatories are the following:

Table 2 – Communities of interest per observatory

Community	Knowledge Hub	CapO	TechO	MFSO	ELSO
Policy, LEAs, Industry, R&I Community	CERIS Expert Group	X	X	X	X
LEA/Police Authorities	Europol Innovation Lab / EuCB / EACTDA/ ENLETS/ ENFSI / EPCC / EMPACT/ INTERPOL Innovation Center	X	X		
Industry	EOS Working Groups		X	X	
RTO	EARTO Security & Defence WG		X		
Standardisation	Certification and Standardisation entities' Workshops and working groups		X	X	X

These communities of interest have been redefined during task T4.2 as explained in section 3. Also the concrete list of Knowledge Hubs and their relationship with the observatories is further elaborated in Section 3.

Each observatory will ensure **at least 1 meeting every 6 months** period with the relevant Knowledge Hubs for mutual update on matters of common interest.

The Knowledge Observatory leaders will represent the Observatory in the direct interactions with external knowledge hubs and stakeholders, with the support of other project partners when needed. Such interactions will be monitored by the Inter-Observatory Coordinator (TX.2) and arranged in collaboration with tasks TX.3 (liaison with LEA Community) and/or TX.4 (Liaison with Industry community).

Despite the direct relationship established between the observatories and the Knowledge Hubs, the outcomes delivered via the different products may be of relevance for the whole FCT community and, thus, respective dissemination of outcomes will be considered. The public or restricted nature of these outcomes will be decided on a case by case basis.

The strategy to convey information to the different communities of interest has been drafted under Task T4.3 and explained in Deliverable D4.2, including publications in ENACT website and social media, availability to ENACT products and resources, communication channels for

handling sensitive information, periodic workshops and meetings, participation in external activities, etc.

It should be noted that certain stakeholder groups within the knowledge hubs have already defined and structured some interest areas. In order to increase the usefulness of the products delivered to these groups, ENACT will ensure that the information contained in such products and in the Structured Knowledge Base in general can be easily mapped to the interest areas. Currently, the interest areas of two stakeholder groups, members of the LEA community, have been identified. These are the following:

- Interest areas of the **EUCB**:

- AI;
- Ethics and Technology;
- Facial recognition technologies;
- Darknet monitoring tools;
- Extended reality;
- Forensic profiling of fraudulent documents;
- Online policing;
- Satellite imagery;
- Secure communications;
- Speech and text analysis;

- Interest areas of **ENLETS**:

- Digital Workplace;
- Public Order;
- C-UAS;
- Financial Investigations;
- Operational Centres;
- Green Policing.

During the implementation cycles, it will be the responsibility of tasks TX.3 and TX.4 to maintain an updated list of the Interest Areas of the Knowledge Hubs (when known), and to map these interest areas to the Knowledge Base structure in order to facilitate the identification of information relevant to each of these Hubs.

As stated in the ENACT Grant Agreement, the measurement of the perceived usefulness of the ENACT products (see section 2.4) by the external stakeholders is one of the project's Key Performance Indicators (KPI.2.8). To get this feedback, the recipients of the ENACT products will be timely consulted on the perceived usefulness of the delivered product. The rationale behind the consultation will be based on the SSRI-01-02 topic itself, when it says that "[Commission and Member State] experts require high quality, reliable and timely evidence to support their assessments, but information is often scattered, hardly visible and requires bespoke processing for the detection of patterns and for the generation of actionable intelligence. In other cases, it is simply not presented in the right format to unveil its value.". Based on this, the recipients of ENACT products will be asked to reply to the following question:

Please rate from 1 (no contribution) to 5 (excellent contribution) how the following features of the report contribute to its usefulness:

a. The quality of the report

b. The reliability of the report

c. The timeliness of the report

d. The format of the report

e. The value of the information contained in the report (to the respondents organization and their perceived value to the FCT community).

All the replies compiled during the project will be aggregated to extract an average perceived usefulness which, as stated in the Grant Agreement, is expected to be above 3 following the scale defined above. The perceived usefulness will be monitored during the project in order to implement corrective measures in case the rating falls below the targeted threshold.

2.4 Products

The Observatories will acquire and classify sufficient information to allow the periodic elaboration of the Key Exploitable Results 2 to 5 by the Inter-Observatory Coordinator.

According to the ENACT proposal, the following products need to be produced during the project under the RESEARCH pillar:

- Periodic FCT Maps (KER2) -> KPI2.2 = 5
- Flash Knowledge Reports (KER3) -> KPI2.3 = 25
- Advanced Expert Reports (KER4) -> KPI3.7 = 6
- FCT State of play policy report (KER5) -> KPI2.5 = 3

The **Periodic FCT Maps (KER2)** will provide a comprehensive summary of all the information collected by the observatories during the previous 6 months on FCT-relevant security threats, police functions and policy (Capability Map – CM), on product/services, ongoing research and scientific breakthroughs (Technology Map – TM), on funding, procurement and standardisation opportunities (Market Map – MM) and on Ethical, Legal & Societal issues (ELS Map – EM). The FCT Maps will also include specific insights on the feedback obtained from the interactions of the Observatories with the different knowledge hubs and stakeholders (e.g. via meetings, workshops, surveys, consultations, etc.)

The precise content of the maps is still to be defined based on the data sources that will be collected (see Section 2.8) and on the final implementation of the Structured Knowledge Base (see Section 2.6). A first approximation to the content of the maps could be based on summarising the different types of contents that are available at the Knowledge Repository at the time of the reporting. According to the data categories contemplated in section 2.8 below, the structure of each FCT Map could be the following:

- **Projects map**
- **Practitioner Reports map**
- **Policy map**
- **News and media map**

- **Scientific literature map**
- **Stakeholder feedback map**
- **Events map**

This structure might change based on the final content types defined for the Structured Knowledge Base.

The Maps will offer a summary of the Observatories activities during the corresponding period and also factual data, statistical information, time evolutions and highlights, but not advanced analyses. All the information presented in the maps should be directly derived from the information stored in the Knowledge Repository and processed by the Observatories.

The **Flash Knowledge Reports (KER3)** will be short and quick reports built on demand. In general, these reports will have a focus on one policy, threat, function or technology (i.e., the driver) and will connect it with the other dimensions monitored by the observatories building on the information that is readily available in the Structured Knowledge Base. In essence, the FKRs will be a documented outcome of an expert search in the ENACT knowledge base. The precise content of the FKRs is still to be defined based on the information that is available at the SKB, however, a first approximation to the content of the FKRs could be the one shown in the following example:

FKR on Cybercrime – Use of Cryptocurrencies

1. **Scene setter**
    a. Description of the key topic to address
    b. ENACT Knowledge base statistics and time evolution
2. **Policy view**[6]
    a. Policy landscape
    b. Policy trends
        i. FCT policy
        ii. R&I policy
3. **Technology view**
    a. Summary of technology view
    b. Commercial/Operational products view
        i. Featured product(s)
    c. Projects view (EU & MS, R&I and Development)
        i. Projects summary
        ii. Techs addressed by projects
        iii. TRL assessment
        iv. Featured project(s)
    d. Science view
        i. Featured scientific papers
4. **Market View**
    a. Summary of Market view
    b. Market size
        i. Investment in relevant R&I
        ii. Investment in EU procurement
    c. Relevant market actors
        i. Participants in R&I projects
        ii. Product suppliers

[6] In this example, the policy view is the driver (Cybercrime Use of Cryptocurrencies). Therefore, it goes first in the list. The other views will address technology, market and ELS, in connection with the driver.

iii. Technology sovereignty assessment
   d. Review of relevant funding opportunities
   e. Review of tender opportunities
5. **Ethical, Legal, Societal View**
   a. Summary of ELS view
   b. Critical ethical and societal issues
   c. EU and MS legal framework
6. **Highlights:**
   a. Latest news (max. 1 month old)
   b. Relevant events (max. During next month)

With the aim to foster the collaboration with other R&I project with analytical capacity, depending on the scope of each flash report, the possibility to include an additional section with foresight inputs on the matters addressed will be explored. These inputs could be provided by the AHEAD[7] project, which periodically deliver foresight analysis on a variety of matters.

The following restrictions shall apply to the elaboration of the Flash Reports:

- **Requesting entity:** These reports shall be requested solely by the designated point of contact at DG HOME. DG HOME might convey requests coming from other entities connected to the EU-funded FCT R&I community, notably requests coming from the Knowledge Hubs identified by ENACT.
- **Request procedure:** The request will be channelled through the Inter-Observatory Coordinator through a specific email address enabled by the project to that effect. Upon receipt, the IOC will liaise with the four Knowledge Observatory Leaders for the production of the report. The request should include a short description of the scope of the report, including the driving policy, threat, function or technology where the focus should be on. It should also mention if the report is to be considered Public or Restricted (and if so, the stakeholders who may have access to it e.g. PUBLIC, RESTRICTED (Group)). By default, these reports will be considered Public.
- **Extension of the report:** The report should be concise, with a maximum of 5 pages length (excluding front page, blank pages, and pages including references, acronyms and content tables) with a possibility to add annexes with additional information as needed. The content will be structured in the sections described in the example above, each with the following approximate length:
  - Scene setter (0,5 pages)
  - The policy/operational view (1 page)
  - The technology view (1 page)
  - The market view (1 page)
  - The Ethical, legal societal view (1 page)
  - Highlights (0,5 pages)
- **Delivery time:** The report shall be delivered in a maximum of four weeks, being the concrete date of delivery confirmed to the requesting party no later than **five working days** following the receipt of the request. In the event that the ENACT consortium

[7] AHEAD. Project details. Available at: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/org-details/999999999/project/101121338/program/43108390/details

considers that the SKB of ENACT does not have sufficient information to produce a valid report, the delivery time might be extended or diverted to a different ENACT analytical product (e.g. Analysis Paper or Advanced Report by External Experts). This will be notified to the requesting entity through the formal channels no later than five working days following the receipt of the request.

If no requests to produce FKRs arrive, the IOC might decide to produce FKRs on topics decided by the ENACT consortium with the aim of achieving the minimum deviation as possible from the number of FKRs set as an objective for the overall project (25). However, the lack of requests might have an impact on the number of FKRs finally delivered.

Other types of Flash Reports might be considered if needed to swiftly report to some stakeholders about matters or events that might be of interest at a concrete moment. In these cases, the structure of the report might differ from the one proposed above and will adapt to the nature of the information contained.

In addition to the above, the Observatories may produce **Analytical Reports** on aspects that require further analysis beyond what is offered in KER2 and KER3. The observatories, based on the information available in the SKB and the discussions held with the relevant Knowledge Hubs, will propose a list of analytical reports of interest to be produced at each implementation cycle. The first ENACT Analytical report was already delivered on the 22/11/2023 and will be made available publicly through the ENACT website[8].

Those aspects that fall beyond the knowledge, skills and resources of the ENACT partners, shall be addressed in the **Advanced Reports by External Experts (KER4)**. The experts who will elaborate those reports will be facilitated by the ENACT External Collaboration facility set up under Work Packages 8, 9 and 10 (Task Z.3). Experts may request access to the information collected by the Observatories in the Knowledge Repository in order to complete their analysis, thus the collaboration of the Observatories may be required during the elaboration and the peer-review of the reports.

The Advanced Reports by External Experts shall:

- be clear and concise (max. 30 pages, additional information may be included in an annex);
- be written in English and in non-technical language (i.e. understandable for non-experts);
- use evidence/arguments to support statements/conclusions;
- not contain EU classified or confidential (intellectual property right protected) information;
- require no more than 20 days of work for the expert
- be submitted in less than 2 months from the date of the formalisation of the collaboration agreement with the expert.
- Respect all confidentiality and impartiality terms set for each particular report.

Also with the aim to foster collaboration with other R&I projects, the possibility to forward analysis requests to such projects or to seek the contribution of other projects to the elaboration of certain analyses will be explored. Network projects or projects such as AHEAD

[8] "FCT R&I: An analysis of EU priorities 2014-2024)"; ENACT Analytical report #1; 22/11/2023

could be considered as candidates. The selection of projects will be carried out by the observatories once the analysis requirements are defined at the beginning of each implementation cycle.

Finally, the **Annual State of Play FCT Policy Reports (KER5)** were conceived in the ENACT proposal to provide insights and recommendations to EC services in support of the FCT policy and R&I programming. Given that KER2, KER3 and KER4 will also serve that purpose, the scope of the Annual State of Play FCT Policy Reports will be reformulated, being its final purpose to:

- Condense insights and recommendations derived from products delivered in the preceding 6 months period (notably from Flash Reports and Analytical Reports)
- To compile analysis carried out by ENACT to support CERIS FCT workshops, events and discussions, including discussions held among the FCT experts group, and other FCT R&I events organised by the Commission such as Project2Policy events or the SRE.
- To summarise outcomes and recommendations issued after CERIS FCT workshops, events and discussions, and other events organised by the Commission in support to FCT R&I such as Project2Policy events or the SRE.

In order to achieve this, ENACT guarantees the participation of at least one of its members in every CERIS FCT workshop.

Given that the Annual SoP FCT Policy Reports were conceived strictly as a policy support product, and noting that some of the discussions that will feed these reports are restricted to a limited audience, the Annual SoP FCT Policy Reports will be restricted only to Commission services.

The products generated under the RESEARCH pillar of ENACT will be timely shared with the concerned stakeholders and interested parties, as explained in section 2.3. For that purpose, and depending on the public or sensitive nature of the product, different channels of dissemination will be used, as contemplated in the Communication and Dissemination strategy presented under deliverable D4.2. In addition to that, the products will be compiled at the end of each reporting period (Implementation cycle) in the project deliverables D5.2/3, D6.1/2, D7.1/2. Therefore, the content of these deliverables will be:

- ENACT Activity Reports D5.2, D6.1, D7.1
  - Report with a compilation of all the findings, outcomes and recommendations in the 4 Pillars of activity: KER2, KER3, KER4, KER5
  - Delivery dates: M12, M24, M36
  - Dissemination level: SEN
- ENACT Annual Reports D5.3, D6.2, D7.2
  - Public Report with disclosable information about the network activity and outcomes.
  - Selection of public inputs from D5.1, D6.1, D7.1
  - Dissemination level: PUB

2.5 Functioning

The functioning of the observatories can be structured in three stages of planning, operation and reporting. These stages will include a number of activities that will serve to streamline the conceptual cycle of Acquire-Classify-Measure-Visualise explained at the beginning of section 2.

The planning of the Observatory activities shall be done by the Observatory Leaders at the beginning of each Implementation Cycle. The planning shall include at least:

- An updated list of data sources to monitor;
- An assignment of data acquisitions to contributors;
- Identification of relevant external events per Observatory, recording of planned ENACT representation at those events in a Communications and Dissemination Log[9] and coordination with CDE coordinator as needed;
- A planning of workshops with Knowledge Hubs and direct interactions with FCT community during the Implementation Cycle, including:
    - ENACT meetings and workshops;
    - ENACT questionnaires and surveys ;
    - External R&I project activities;
    - External events, notably those of the CERIS FCT community;
    - Exhibitions and fairs -with special focus on MS events.
- A planning and definition of the products that will be delivered during the implementation cycle, notably of Flash reports, analytical reports and advanced external experts analysis)
- A mapping of interest areas of Knowledge Hubs to the ENACT Knowledge Base in collaboration with Tasks TX.3 and TX.4, and relate it to the expected products for the cycle.
- An assignment of contributions from contributors to the elaboration of ENACT products.

The results of the planning will be recorded in the Detailed Task Workplan (DTW) files for tasks TX.1 to TX.4. These DTW files. A template of such file is included in Appendix E.

The operation of the observatory will include at least the following tasks for the Observatory Leaders and contributors:

Table 3 – Tasks to be carried out during observatory operation stage

Task	Leaders	Contributors	IOC
To introduce information available at the data sources in the Knowledge repository and classify it according to the established categories as part of the Structured Knowledge Base.	X	X	
Propose new data sources to monitor	X	X	
Update the acquisition plan	X		
Data curation	X	X	X

[9] The communication and Dissemination log will be available for internal use. Relevant events recorded in that log will also be announced through the ENACT website calendar. For more information about the ENACT website, please refer to deliverable D4.2.

Knowledge Base content moderation	X		
Interaction with Knowledge hubs and networking coordination	X		X
Elaboration of flash reports on demand	X	X	X
Definition of possible white papers and expert reports	X		X
Elaboration of analytical papers	X	X	x
Elaboration of Annual SoP FCT Policy Reports	X	X	X

Note that some of the above tasks should be conducted in coordination and under supervision of the Inter Observatory Coordinator.

During the reporting stage, the observatories shall mainly contribute to populate the Periodic FCT maps. The maps are produced every 6 months, so during the test implementation cycle there will only be one FCT map at the end of the cycle, while in the full Implementation cycles there will be also an intermediate one.

Beyond the Periodic FCT maps, during the reporting period the Observatory leader in collaboration with the contributors shall compile a list of recommendations for the next implementation cycle in order to improve the functioning of the observatories and the quality of the delivered products.

2.6 Structured Knowledge Base (SKB)

As aforementioned, ENACT's observatories will collect, classify, aggregate, curate and process information pertinent to each observatory in a Structured Knowledge Base (SKB) and appropriately disseminate them to interested parties through a dedicated Knowledge Repository (KR).

Although the terms may be used interchangeably in some occasions, it is important to clarify and distinguish the two terms. To this end, the Structured Knowledge Base (SKB) pertains to the classified and processed outputs of ENACT's Research Pillar and its observatories, while the Knowledge Repository (KR) is the digital container in which the SKB will reside. To this end, the KR essentially pertains to a CDE instrument, therefore its strategies and requirements are described in deliverable D4.2.

Subsequently, the requirements and definitions of the SKB have been set during this period, as follows:

- The contents of the SKB should be organized and characterised (tagged) by finite and structured metadata;
- This characterisation must cater for the following information: mandatorily, the content item type and provenance; optionally, the target audience; most importantly, contextual metadata that will adequately describe the subject(s) of the resources/assets accumulated in the SKB and facilitate search and retrieval of the data within the KR;
- Contextual metadata must either directly use the EU Security Taxonomy (as described in Section 2.7) or have concrete, transparent and direct mappings to it;
- Primary source data will be included in the SKB as qualified references and will not pertain to an exhaustive catalogue of all relevant resources, but rather to a curated

representation of the most indicative, inclusive, prominent (scientifically, technologically, market-wise, usability/popularity-wise) and current assets pertaining to particular topics of, at least, the EU Security Taxonomy.

More specifically, the SKB must cater for specific aspects regarding knowledge interoperability, re-usability, findability (on the contents level) and ethics:

- *Interoperability*:
  - Where possible/applicable, the SKB contents must abide to standards and standards-based formats, such as CERIF[10] and OpenAIRE[11];
  - Define and follow a set of standardized metadata vocabularies (taxonomies, categories) for the characterization of the type, provenance, subject and potentially targeted audience of SKB's contents, such as the Dublin Core ontology[12], the CERIF vocabularies, the EU Security taxonomy, etc.
- *Re-usability*:
  - The SKB must be explicitly licenced, with a license that allows the target audience to consume and re-use its contents. To this end, the public version of the SKB, will be licenced as Creative Commons Attribution 4.0 International (CC BY 4.0[13]), while any potential protected version will follow the appropriate licensing scheme that derives from the encompassed contents' requirements;
  - Maintain qualified references for every content item, that allow or promote mappings to other data, with special regard to provenance;
  - Conclude to a specific maintenance time-plan (in conjunction with the KR) and appropriate migration considerations beyond this time-plan, if needed.
- *Findability*:
  - Again, an interconnected action pertains to the use of standards for the characterization and publication of the SKB and its contents. The public version of the SKB must be published as Open Data, while the public and a potential protected version must be published in adherence to the FAIR Data Objects (FDO) model[14];
  - To this end, clear versioning of the SKB as a whole, predictable digital identifiers for its assets and, as aforementioned, standardized and searchable metadata are mandatory mechanisms for the publication of the SKB.
- *Ethics*:
  - All published content must adhere to the ethics and legal framework of ENACT, following supervision of the Ethics and Legal manager (KUL), including monitoring the dissemination level of the assets.

In conclusion, the SKB will encompass (a) primary source data, acquired and classified by the CapO, TechO, MFSO and ELSO, with accompanying information such as a digital identifier (where applicable), provenance, type, intended audience, source (as qualified reference),

[10] Common European Research Information Format (CERIF), **Main features of CERIF.** Available at: https://eurocris.org/services/main-features-cerif
[11] OpenAIRE (Horizon 2020) website available at: https://www.openaire.eu/
[12] DublinCore website available at: https://www.dublincore.org/
[13] Creative Commons. **Attribution 4.0 International** – CC By 4.0 DEED. Available at: https://creativecommons.org/licenses/by/4.0/deed.en
[14] FAIR. (2022). **FAIR Digital Object Framework Documentation**. Working draft available at: https://fairdigitalobjectframework.org/

collection method, creators/authors, level of curation, rights and licenses, content-related metadata; (b) secondary data, produced by the ENACT consortium, including reports, maps and deliverables, with accompanying information such as the full resource, date published, type, intended audience, creators/authors and contributors, level of curation, rights and licenses, OPENAire mapping/linking, content-related metadata.

The metadata collected in the SKB shall also serve as a source of analytics to measure the impact of the four observatories based on the inputs that they collected and the outputs they helped to produce, thus ensuring a comprehensive view of their effectiveness.

2.7 Tools

The observatories will ingest information from heterogeneous sources, ensuring a broad and permanent surveillance of historic data but also on main trends of today and the near future. The sources to be considered by each observatory may vary in function of the specificities of each knowledge area (see section 2.8 Data Sources).

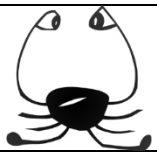
As a regular practice, the planning of data acquisition to be carried out at the beginning of the implementation cycle will also include the identification of tools to be used by the observatory members to detect observations of interest. Given that a majority of sources (from the ones currently included in the data sources list, Section 2.2, Appendix B) are available via internet, the use of online data acquisition tools which can automate to some extent the search process will be very relevant[15]. In this regard, free and open source web-based news feed (RSS/Atom) readers and aggregators will be prioritised. Nonetheless, as explained above, the data mentioned will be refined and reviewed by the ENACT consortium members according to the functions of each member.

The following table shows a set of tools that can be used by ENACT partners to acquired data from the identified data-sources.

Table 4 – On-line data acquisition tools

Name	Logo	Type	URL
Tiny-Tiny RSS		news feed (RSS/Atom) reader and aggregator	https://tt-rss.org/
Google Alerts	Google alerts	Web change detector	https://www.google.es/alerts
Feedly	feedly	News reader	https://feedly.com/news-reader
Inoreader	inoreader	News reader	https://www.inoreader.com/es/
Flipboard		News reader	https://flipboard.com/
Deltafeed	DELTAFEED	Web change detector	https://bitreading.com/deltafeed/
Changedetection.io	CHANGEDETECTION.IO	Web change detector	https://changedetection.io/?src=github

[15] Note that these automated tools are related to the data acquisition, not the data classification. Also, any data automated collected will be supervised/reviewed by a human.

Name	Logo	Type	URL
Kill the newsletter		RSS Generator	https://kill-the-newsletter.com/
PolitePol		RSS Generator	https://politepol.com/en/
Feed Rinse		RSS Generator	http://feedrinse.com/index-old.php
RSS Bridge		RSS Generator	https://rss-bridge.org/

The information acquired by the observatory will be classified in order to facilitate the findability but also the exploitability. The classification scheme will ensure traceability of the acquired information to the EU Security Market Study FCT taxonomy in order to create a more structured and harmonised body of knowledge that can be shared, exploited and compared.

The EU security taxonomy is one of the main outcomes of the EU Security Market Study commissioned by DG HOME with the aim to facilitate the dialogue with the EU security industrial base[16] and to provide a comprehensive view on the dynamics of the market in terms of value, supply and demand, competition and trends[17].

The taxonomy is a first step towards a functioning, actionable way to create a common language concerning European civil security. It provides a comprehensive and detailed reference for security products and services built around:

- the four security areas (L1) with their respective sub-areas (L2 and L3)
- The security functions that a given product or service enables or supports (i.e., functional areas)

The policy dimension of the taxonomy is structured in four main areas, replicating the DG HOME part of the Cluster 3 Work Programme. Each policy area is then disaggregated into two more levels.

[16] European Commission Staff Working Document SWD (221) 422: Enhancing security through R&I

[17] European Commission. **EU security market study**. Available at: https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security/eu-security-market-study_en

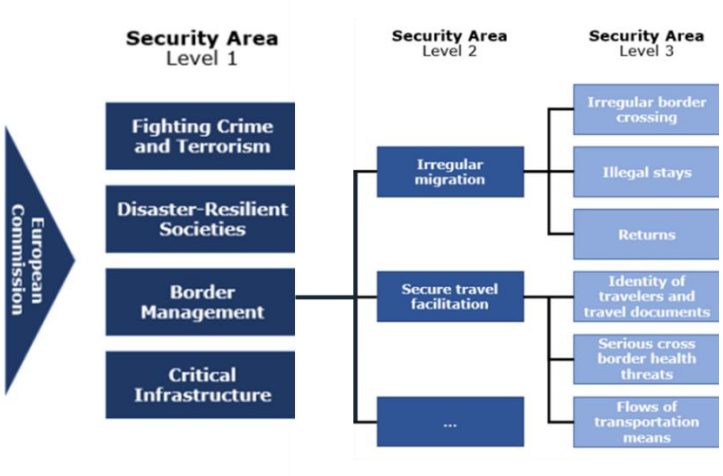


Figure 3 – Security Taxonomy – Policy dimension structure

The FCT area breaks down into the following Level 2 and Level 3 sub-areas:

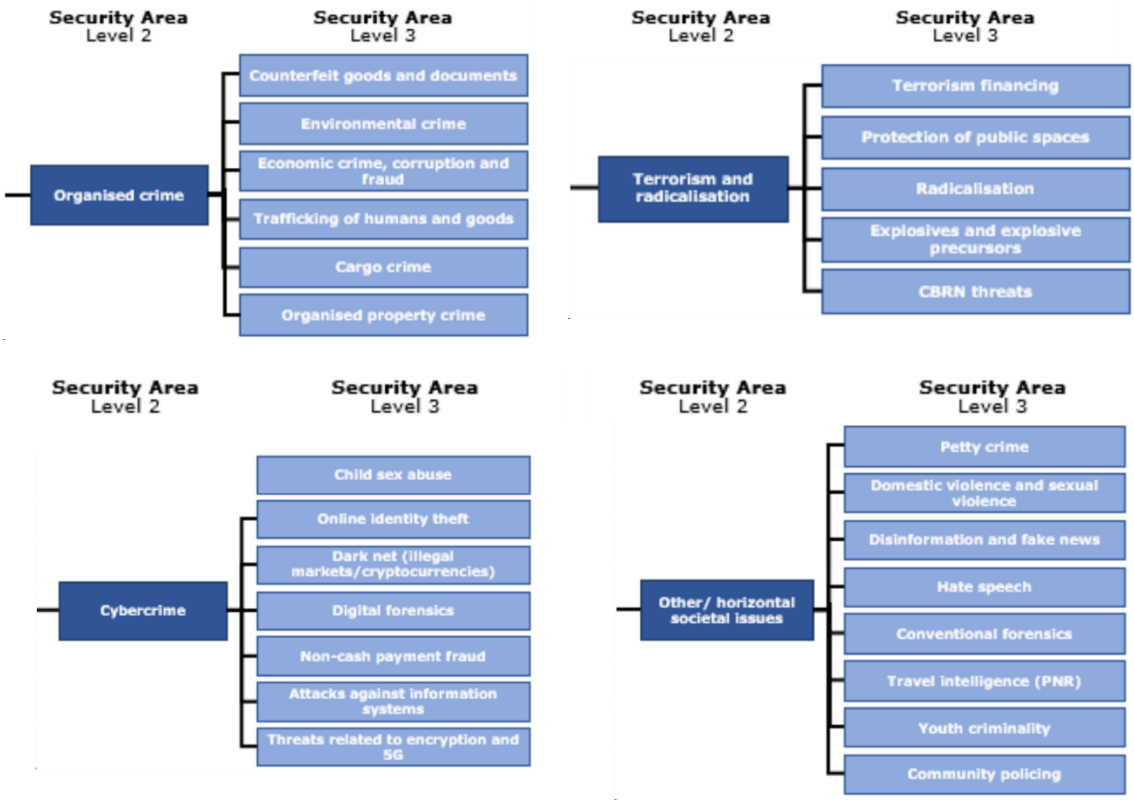


Figure 4 – Security Taxonomy – FCT Policy dimension

The Functions dimension of the taxonomy is not policy-specific. It includes the following categories of police functions.

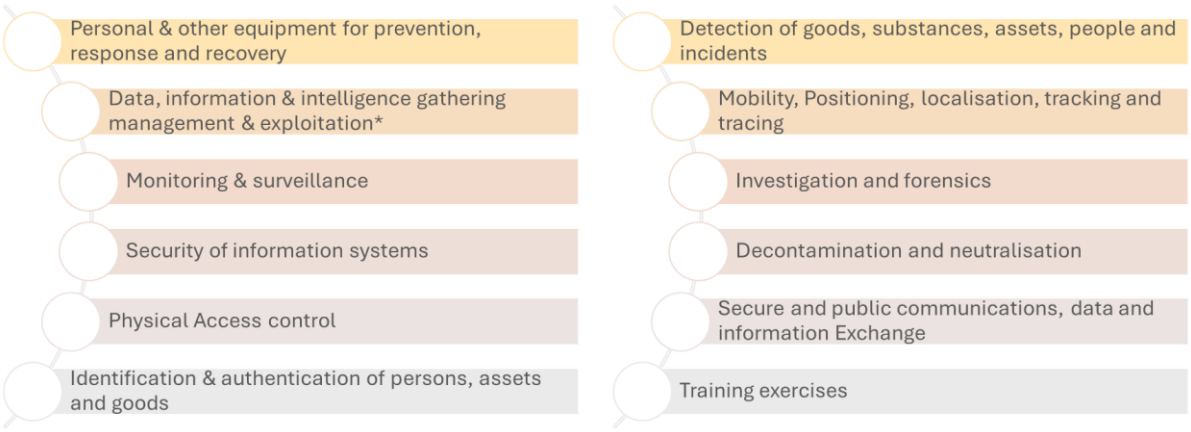


Figure 5 – Security Taxonomy – Functions dimension

Likewise, the technology dimension is not policy-specific. It contains more than 500 technologies in the form of products/services structured in four levels of aggregation. The following table shows only the higher level technology areas.

Technology areas	
Access control/authorisation (building access, system access, etc.)	Laboratory equipment for gathering and forensic analysis of samples
Alarm/warning systems	Healthcare / medical equipment
Data analytics	Monitoring tools and services
CBRNE detection and neutralisation products	PPE/Safety equipment
Data storage and exchange	Screening & detection
Digital forensics	Search devices and tools
Digital security products and services	Specialised management & control systems
Facilitation systems and secure databases	Surveillance systems
General equipment	Tracking, navigation and guiding systems, equipment and tools
Guarding and physical protection (non-human)	Training & Simulation
Internet-based investigation	Conflict management / Use of force
	Critical communications, Interoperable communications

Figure 6 – Security Taxonomy – Technology dimension

The full structure of the taxonomy to be considered under ENACT is attached to this document in Appendix A.

As expressed by the Commission, the taxonomy shall be further refined through its practical use and cyclical updating. It is therefore the intention of ENACT to use the taxonomy for its activities and propose changes to DG HOME at the end of the project.

2.8 Data sources

In order to facilitate data acquisition and maintain detailed reference to sources for later use within the SKB's classification scheme, a concrete list of attributes has been defined for the characterisation of the data sources to be acquired, classified and exploited by the Observatories, as it follows:

- **Source of information:** Name of the source
- **URL:** URL where the source can be found (if any)
- **Relevance:** Relevance of the source to the field of interest addressed by each knowledge observatory. The relevance shall be expressed as:

  - High relevance
  - Medium relevance
  - Low relevance
- **Category:** One of the following:
  - **Project results:** Results delivered by FCT relevant projects funded by EU programmes (mainly Horizon and ISF). These will mainly refer to results that are publicly available directly in CORDIS (Fact sheet, results in brief and reporting) or accessible through CORDIS (Results = public deliverables)
  - **Practitioner Reports:** Reports delivered by relevant stakeholders on a punctual or periodic basis, with priority to those reports issued by the reference Knowledge Hubs or members of those Knowledge Hubs.
  - **Public database:** Data, information and business intelligence publicly available, notably, but not exclusively, through the Funding and Tenders Portal and the Horizon Dashboard.
  - **Policy papers and updates:** FCT relevant EU Policy available through DG HOME website
  - **News and media:** FCT relevant news in global media and through the communication and dissemination channels of EU-funded projects.
  - **Scientific material:** FCT-relevant Scientific papers, conference procedures, etc.
  - **Consultation result:** Reported results of ad-hoc initiatives launched by the Observatory in order to gather targeted views from the relevant stakeholders using surveys, open consultations, interviews, etc.
  - **Other**
- **Type:** One of the following
  - Document
  - Website
  - Audiovisual
  - Database/Dataset
  - Other
- **Language:** Indicates the language in which the source is written
- **Dissemination level**
  - Public
  - Limited
- **Classification level**
  - Open
  - EUCI
  - Other
- **Acquisition plan:** Periodicity of the acquisition/update of the source and incorporation to the SKB.
  - Punctual / On occasion
  - One-time (during the project)
  - Once per Implementation Cycle
  - Annually
  - 6-monthly
  - Monthly
  - Weekly
- **Comments:** any other comment relevant to characterise the source of information.

An initial set of data sources has been compiled and characterised to be used during the first test implementation cycle. This has been attached to this document in Appendix B. The data sources list will be updated and extended by the Observatories throughout the implementation cycles.

Also in relation to the data sources, the consortium has made a first analysis of all the FCT projects funded under the H2020 and Horizon Europe programme. An exercise has been done in order to match every project with the topic from which it emerged, and assign a correlation to the EU security market study taxonomy, following the findings of the first ENACT analytical report. The mapping of projects to the taxonomy, far from being perfect, represents a useful baseline information, as it will serve to narrow down the search of relevant projects in relation to particular thematic areas of interest, for example for the elaboration of Flash Reports. The mapping of projects to the taxonomy is attached in Appendix C.

3 ENACT Networking Tools

The goal of the ENACT project is to set-up a Knowledge Network that is able to channel all the resources available inside and outside of the consortium and put them at the service of the FCT R&I community.

ENACT will build on a strong NETWORKING pillar, identifying the role of each actor in the Security R&I ecosystem and interacting with them according to their mandates and objectives. The NETWORKING pillar will support and facilitate the work of all the other ENACT pillars, namely the RESEARCH, COMMUNICATION, DISSEMINATION AND EXPLOITATION, and COOPERATION pillars, by organising and providing a network of relevant FCT related knowledge hubs, organisations and expert individuals in support of the pillars objectives and goals.

ENACT is aware that the community of FCT R&I stakeholders goes well beyond the boundaries of the project. The objective is therefore to act as a network enabler and foster the exchange of knowledge between the wider network entities, as well as amplify the outcomes of these interactions. The work of the Network is outward-looking and will put its resources at the service of the community, thus avoiding that the knowledge creation process contemplates only the views of the members of the consortium and of entities with a formal commitment with the project while leaving other external actors unheard. It shall, therefore, be a major objective to establish and maintain strong ties with the communities of interest in the FCT R&I domain, including but not limited to: Policymakers, LEAs practitioners, Industry & Small and Medium-sized enterprises (SMEs), Research & Technology Organisations (RTO), Civil Society Organisations, International/Non-EU LEA organisations and Academia/Experts. ENACT will also connect to relevant other EU funded projects.

This section about the NETWORKING pillar will define the working tools, methods and processes of the networking activities. It reflects the results of T4.2 and will define a strategy and set-up of necessary methods and tools to ensure ENACT's presence in the most relevant FCT Knowledge Hubs, representing the six communities of interest:

a) FCT Policymakers

b) FCT Practitioners

c) FCT Industry and RTO's

d) Civil Society

e) International non-EU LEA/Police Authority

f) other EU projects

It will be the role of Tasks TX.3 and TX.4 in Work Packages 5, 6 and 7 to implement, maintain and update this ENACT Networking strategy in close collaboration with the Observatory leaders and the Inter-Observatory Coordinator.

3.1 Defining the ENACT Stakeholder map

The NETWORKING pillar will support and facilitate the creation of a comprehensive and representative networking environment for all pillars. The project will neither connect with every

single stakeholder nor absorb as many as possible under its direct constituency. Its strategy is to connect the project with the main, and already existing, Knowledge Hubs and organisations from the FCT ecosystem.

In establishing the KER1 (FCT R&I Stakeholders map) in T4.2, the NETWORKING pillar is constructed and defined as the relevant knowledge hubs and organisations that belong to the abovementioned FCT community of interests.

The key established/formal groups/entities that represent all the different communities of interest will be targeted as part of the ENACT stakeholder map.

The main EU FCT R&I Knowledge Hubs to which the ENACT partners have direct access are the following (at start of the project):

Table 5 – Identified knowledge hubs at the start of the project

Community of interest	FCT Knowledge Hubs	ENACT partner with direct access
Policy, LEAs, Industry, R&I community	CERIS expert group	Individual experts appointed by CERIS hold key positions in PJ, ESMIR, FRMDLI, NP, ENG, CENTRIC, CERTH, VICOM
Policy	DG HOME	All
LEA/Police Authorities	Europol Innovation Lab / EuCB / ENLETS/ ENFSI / EPCC / EMPACT/ INTERPOL Innovation Center	PJ, ESMIR, FRMDLI, FIMOI, NP (chair EUCB; chair ENLETS; INTERPOL liaison)
Industry	EOS	EOS, ENG, CENTRIC, VICOM
RTOs	EARTO Security & Defence WG	INOV, VICOM
R&I Community	EU FCT R&I projects (H2020, HE, ISF)	All
R&I Community	EACTDA	PJ, ESMIR, FRDMLI, NP, CERTH, INOV, VICOM
R&I Community	Security Networks of Practitioners (NoP): I-Lead, ILEAnet. Security Knowledge Networks: EU-CIP	PJ, ESMIR, *FRMDLI (ILEAnet Coordinator)*, FIMOI, NP *(I-Lead Coordinator),* EOS, ENG (*EUCIP Coordinator*), KUL, INOV, CERTH
CEN Standardization	CEN / CENELEC Workshops in Defence and Security	VICOM, ENG
Ethical & Legal community	Ethical, Legal, AI related R&I projects, initiatives in FCT	AP4AI project (*CENTRIC Coordinator*), TAILOR Network (KUL), popAI project (CERTH), ALIGNER, EUHubs4Data (KUL), EDEN (Europol Data Protection Experts Network), UNICRI (KUL)

In the upcoming tasks 3 and 4 of Work Packages 5, 6 and 7, ENACT will continue to connect and interact with these (and potential new) knowledge hubs and organisations in order to build a working relation with them and to guarantee the capture and delivery of knowledge to the whole FCT R&I community considering the types of activities that will be conducted during

ENACT's implementation cycles. When the establishment of formal partnerships with these hubs is required, ENACT will ensure that the terms of those partnerships are in accordance with the Legal and Ethics Framework defined for the ENACT project under deliverable D1.3 (Ethics and Legal Analysis report). Any exchange of data with these hubs or with any other entity addressed as an ENACT stakeholder will also abide with the rules for data management defined under deliverable D1.2 (Data Management Plan).

The ENACT stakeholder map is the main source of ENACT connections with the FCT community as a whole for all ENACT pillars. As mentioned in section 2.3 there will also be a direct link between some of these hubs/organisations and the project's Observatories.

In the following paragraphs the foreseen relations and interaction between the ENACT pillars (and observatories) and the internal roles and responsibilities will be described. It is crucial to coordinate the interactions to prevent multiple overlapping and conflicting interactions from and to ENACT and the Knowledge Hubs.

3.2 Stakeholder map relation with Knowledge Hubs

The clear relation, interaction, and communication between the Knowledge Hubs/organisations and the ENACT project organisation is quite a challenge since:

- Multiple ENACT pillars and observatories (and its ENACT partners/task leaders) have interest in connecting to the same hubs/organisations;
- The hubs themselves may also have multiple topics upon which they are building and collecting knowledge;
- The FCT domain covers a broad pallet of policies and areas of interest. DG HOME has several destinations, EuCB has several strategic and core groups on different FCT topics and ENLETS also focuses on multiple Technology Interest Groups;
- Next to the identified Knowledge hubs and organisations, ENACT also needs to have access to identified experts to support the elaboration of advanced studies related to the tasks for RESEARCH and COOPERATION pillars;
- The CDE pillar will need to reach out to not only the identified Knowledge hubs and organisations but the whole FCT R&I community to support the awareness building and organise events and invitations.

In order to handle these challenges ENACT proposes the following measures to be used and tested in the first test implementation cycle (WP5) and evaluated during and after the execution of the cycle:

- Appoint an ENACT Point of Contact (PoC) related with each identified Knowledge Hub among the partners participating in Tasks TX.3 (Liaison with LEA) and TX.4 (Liaison with industry) of WP5, 6 and 7. This ENACT PoC will participate in the coordination of the interaction between the Observatories and the Knowledge Hubs along with the Observatory Leaders and the Inter-Observatory Coordinator. Meaning each individual Knowledge hub has one coordinating ENACT PoC (not necessarily the same for all Hubs). It may be crucial to also have a counterpart Hub PoC on the side of the Knowledge Hub/organisation. This does not mean that only one ENACT partner is allowed to have contact with that knowledge hub/organisation, but all partners will make sure that any official contact between ENACT and the Knowledge Hubs will respect the functioning procedures defined in section 2.5 and the provisions set out in the Networking Strategy;

- To facilitate an overview of all interactions, connections and related communications and exchanged knowledge, the partners involved in tasks TX.3 and TX.4 of WP5, 6 and 7 will setup a private, non-publishable, NETWORKING logfile in the internal project filesharing repository[18] (password protected), where all activities between ENACT and the Knowledge hubs are to be logged;
- This NETWORKING logfile will contain: ENACT PoC; Hub PoC, description of the topic of the interaction; date of the interaction; reference to relevant exchanged and/or discussed document/event/product; possible agreed action points; related KPIs if appropriate. The logfile serves as a communication 'track & trace' trail and as an archive to prevent miscommunication, loss of information shared/discussed and overlap between ENACT and Hub PoC. This system will provide a smooth communication even in case the PoCs are changed/replaced during the course of the project); the logfile will be handled as 'Sensitive' and remain only available for relevant consortium partners as an internal document. The management of said logfiles will be detailed in the updated versions of the Data Management Plan, which will be part of D2.1 and D3.1, to be submitted by M24 and M36, accordingly. It will be defined which partner will have access to each logfile and, if needed, a pseudonymised version of the file will be made available for the consortium partners.
- ENACT will follow the EU security taxonomy (one of the main outcomes of the EU Security Market Study commissioned by DG HOME), with the aim to facilitate the dialogue between the ENACT pillar related activities and the relevant hubs/organisations. In this regard, the partners involved in Tasks TX.3 and TX.4 will, as defined in the functioning procedures set out in section 2.5, maintain a mapping of interest areas of Knowledge Hubs to the ENACT Knowledge Base (notably, but not restricted to, the EU security Taxonomy elements), following the SKB metadata strategies defined in Section 2.6 (e.g. the target audience characterisation), in collaboration with the Observatory Leaders, and relate it to the expected products expected for the cycle.

During the upcoming first test implementation cycle (WP5) these measures will be tested, evaluated and if needed changed for the following two implementation cycles (WP6 and 7).

3.3 Internal procedures and responsibilities

Based on the abovementioned measures, the ENACT internal procedures and responsibilities will be further refined during the test implementation cycle (WP5) in order to have a finalised and consolidated procedure ahead of the full implementation cycles (WP6 and 7). This detailed procedure will be included in deliverable D5.1 and will guide the ENACT partners and the 4 pillars on how to use the ENACT stakeholder map to ensure timely and optimal engagement with the Knowledge Hubs and organisations.

The planning of the periodic interactions and the internal coordination measures that are needed internally (see section 2.5), given the structures and roles defined in the project, will be a crucial part of these procedures and the test phase in the 1st implementation cycle. The internal roles are: Project coordinator, Work Package and task leaders from WP5, 6 and 7, plus each partner responsible for the activity/observatory at hand from RESEARCH, CDE or

[18] This does not refer to the Knowledge Repository, which will not publish such information in neither its public or potential protected forms, but rather to the internal, private, organisational, filesharing repository established within the project, available to and accessible by only consortium partners.

COOPERATION pillar. This is not a hierarchical setup but a collaborative approach to prevent overlapping and conflicting interaction with the Knowledge hubs and organisations.

A monthly NETWORKING pillar coordination team meeting will be monitoring, facilitating, and assessing the Stakeholder map entries and the related progress. This team meeting will be called and chaired by the Inter Observatory Coordinator and run by the leaders of Tasks 3 and 4 in Work Packages 5, 6 and 7.

3.4 The ENACT stakeholder map

Based on the above paragraphs, the ENACT stakeholder map can be visualised schematically as follows:

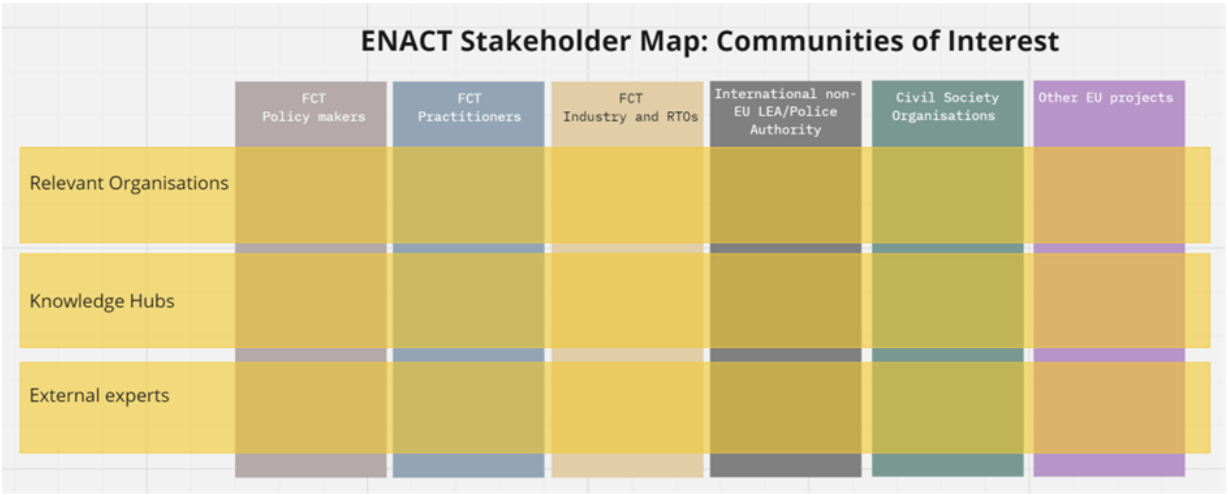


Figure 7 - ENACT's Stakeholder map

The six vertical communities of interest are combined with the horizontal type of connected entity: Knowledge Hub, Relevant organisation and the External experts.

Each of the intersections need to be occupied by preferably minimum of 2 stakeholders.

The Stakeholder map will only reveal the name of the Hub/Organisation/expert organisation. Only in exceptional cases related to external experts the pseudonymised version of their name may be displayed, guaranteeing that the public version of the map will never contain names or contact details of individuals.

At the end of the project and according to the ENACT grant agreement, the following KPIs need to be reached during the project under the NETWORKING pillar:

KPI.1.1. Number of Stakeholders identified: >150;

KPI.1.2. Number of liaisons with EC and EU agencies: >36;

KPI.1.3. Number of liaisons with LEA Knowledge Hubs: >20;

KPI.1.4. Number of liaisons with industrial/scientific Knowledge Hubs: >20;

KPI.1.5. Number of MoUs and interactions established with FCT R&I projects and initiatives: >20 (a template ENACT MoU is attached as Appendix D);

KPI.1.6. Number of consultations/surveys/feedback compiled from external Knowledge Hubs: >20.

Although these KPI's are linked to the NETWORKING pillar, they can only be realised in close collaboration with the other 3 pillars.

To support and facilitate the registration of the ENACT stakeholder community the following spreadsheet "ENACT Stakeholder register" has been developed. All ENACT consortium members are responsible for providing suggestions regarding the stakeholders that should be engaged. In the sheet also the PoC from ENACT and the counterpart is mentioned with relevant contact details. The ENACT register is a private, project internal, non-publishable document, stored only in the internal project filesharing repository (password protected). Following the rules and usage of the dataset, pseudonymisation techniques will be applied whenever possible. Finally, any personal information maintained in these registries shall be deleted timely.

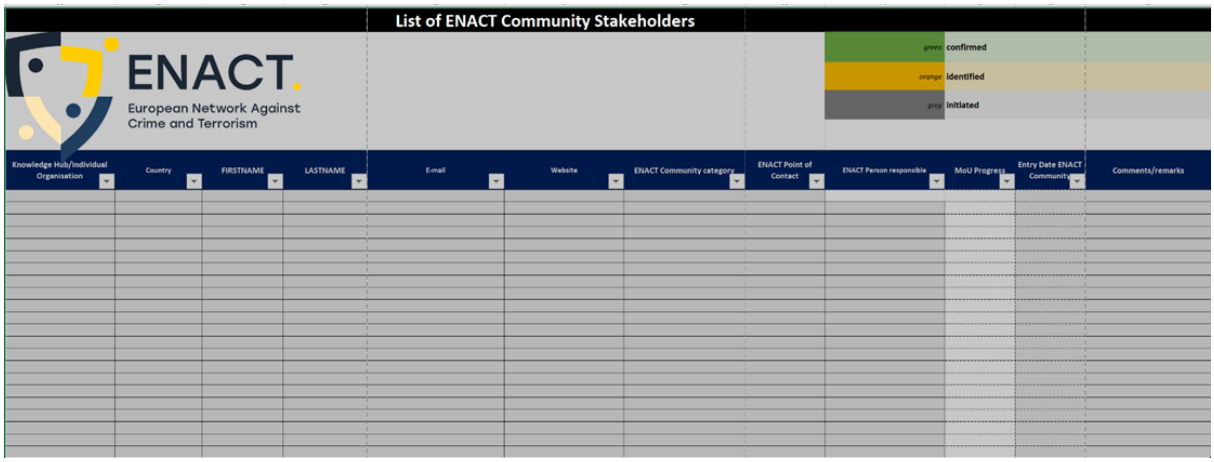


Figure 4 - ENACT Stakeholder register

Together with the ENACT NETWORKING Logfile with all registered interactions, connections and related communications and exchanged knowledge the project can monitor the progress and the compliance to the KPIs for the NETWORKING pillar.

4 Conclusions

This document has set out the strategy to steer the RESEARCH and NETWORKING pillars of ENACT during the three implementation cycles foreseen in the Grant Agreement. The strategy defines the main project structures, actors, functions and resources to carry out the planned work, with the Observatory System as a cornerstone. Putting this strategy in practice will be the responsibility of tasks 1 (Knowledge Observatories), 2 (Inter-Observatory Coordinator), 3 (Liaison with LEA community) and 4 (Liaison with Industry) under the three work packages aimed at implementation, WP5, WP6 and WP7.

The support of the Amplification Actions Work Packages will be crucial in what regards the engagement with the global FCT community, the communication and dissemination of the observatory products, and the cooperation with experts, initiatives and organisations for incentivising the exploitation of FCT R&I results, the validation of innovative technologies, and the generation of knowledge.

The level of detail in this strategy is expected to increase during the test implementation cycle, which will experiment with the concepts proposed, extend the detail of their definition and find aspects where improvement is needed. At the end of the first implementation cycle, an updated version of the strategy will be produced under deliverable D5.1.

Appendix A. EU Security Market Taxonomy

The EU Civil Security Taxonomy aims to create a common language or harmonised terminology, as well as a comprehensive categorisation, for security products and services. The taxonomy provides a comprehensive and detailed reference built around three dimensions: the four **security areas** (Level 1) with their respective sub-areas (Level 2 and Level 3), the **security functions** that a given product or service enables or supports (i.e., functional areas) and the list of over 500 **products and services** grouped in technology areas in three levels aggregation. The following tables show the FCT policy dimension, the functions dimension and the high-level areas of the technology dimension.

4.1.1.1.1.1 FCT Taxonomy – Policy Dimension

FCT Policy Sub-area (Level 2)	FCT Policy Sub-area (Level 3)
Organised Crime	Counterfeit goods and documents
	Environmental crime
	Economic crime, corruption and fraud
	Trafficking of humans and goods
	Cargo crime
	Organised property crime
	Other forms of organised crime
Terrorism and radicalisation	Terrorism financing
	Protection of public spaces
	Radicalisation
	Explosives and explosive precursors
	CBRN Threats
	Other forms of terrorism and radicalisation
Cybercrime	Child sex abuse
	Online identity theft
	Dark net (cryptocurrency)
	Digital forensics
	Non-cash payment fraud

	Attacks to information systems
	Threats to encryption and 5G
	Other forms of cybercrime
Other / horizontal societal issues	Petty crime
	Domestic violence and sexual violence
	Disinformation and fake news
	Hate speech
	Conventional forensics
	Travel intelligence (PNR)
	Youth criminality
	Community policing
	Others

4.1.1.1.1.1.2 FCT Taxonomy – Functions Dimension

High Level Security Functions	Description
Personal & Other equipment for prevention, response and recovery	PPE vehicles, platforms and other equipment for: • first responders during incident response and recovery. Includes special land vehicles, such as armoured vehicles, water cannon systems, etc.; aircraft (planes, helicopters) and un-manned flight systems (UAVs); ships and boats for use by coast guards; emergency equipment such as power generation, temporary shelters, specialist search and rescue equipment (other than for positioning and localisation of persons) (see 'decontamination, and neutralisation for more) • regular security operations (police patrolling, civil protection operations border management), including equipment for deterrence / prevention, e.g. non-lethal weapons, guns, etc.), • Emergency medical support, psycho-social support services.
Data, information & intelligence gathering management, and exploitation	Collection, processing, analysis, management, exploitation and dissemination of data, information and intelligence (e.g. Data fusion techniques including mining, trend detection and optimization analysis) to support, inter alia: • Information analysis for intelligence functions, such as counter-terrorism and criminal intelligence (includes systems that enable /

High Level Security Functions	Description
	support pre-processing of large amounts of data for law enforcement purposes); intelligence for facilitation of travel at border crossing points, i.e. traveller / passenger facilitation, customs risk management systems; • Information management for command & control to facilitate common operational picture between different security actors (within and between departments, regions, nations); • Information support for situational awareness and (intelligent) decision making including through planning and risk assessment, e.g. forecasting, vulnerability and risk and cascading effects assessments, etc.; • Digital forensics, including to track and trace criminal actions in information networks; • IT security incident management.
Monitoring and Surveillance of environments and activities	Large/wide area surveillance of people and vehicles in specific environments (e.g. marine / maritime, air, land/rail borders). Includes monitoring and surveillance of: • Large and small fast boats and underwater vehicles at blue borders; • Manned and unmanned vehicles (air surveillance), e.g. UAVs, light aircraft (linked to ATM systems); • Movement of people and land-based vehicles at regulated and unregulated land borders; • Remote detection of shipping containers Localised / small area surveillance of people, equipment and vehicles in controlled areas such as facilities, critical infrastructure, urban areas, transport and logistic hubs, seaports and harbours, airports and other specified locations. Includes video and other observation and surveillance systems, such as CCTV and video analytics, etc. • Seismic, meteorological, biological and epidemiological monitoring to predict and detect geological hazards, weather-related hazards, dangerous pandemics, etc. CBRN monitoring in Seveso sites. Also includes monitoring of air / water, etc for early detection of CBRN contaminants.
Security of information systems, networks and hardware	Digital systems / ICT hardware, systems and networks, software and hardware security engineering. Includes products for: certification, electronic seals, cryptography, data security and privacy, data loss prevention, data recovery solutions, security of AI systems; use of AI systems to get access to information (security of data mining technologies); infrastructure for secure data storage. Anomaly detection systems, intrusion detection systems; network monitoring systems; malware detection. If we discuss e-access control here, biometrics are missing.
Physical access control (of locations, goods, etc.)	Mechanical access control, barriers, enclosures and physical resilience systems and devices. Includes locks and locking systems, safe, strong boxes, armoured and fire-resistant doors, mechanical seals (and electronic

High Level Security Functions	Description
	seals without tracking), physical perimeter barriers (e.g. fencing and other security barriers), blast proofing, CCTV systems, etc.
Identification and authentication of persons, assets and goods (Other than for tracking and tracing)	Identification, authentication and verification of: • persons for protection against identity theft and fraud, identity management, passenger travel security and verification (e.g. smart cards, biometrics, PIN and chip cards, identity cards, passport systems etc.), • persons for secured access control to buildings and other designated secure areas (sites and places) such as airports and seaports. • persons in crowded spaces (i.e. identification of searched individuals in crowds); • goods and documents to protect against forgery and counterfeiting. • dangerous or illicit materials and substances (drugs, explosives, CBRN) [Note: Distinction with CBRN / dangerous substance detection: identification occurs after a broad substance type has been detected for early warning, a more precise check is done to identify substance type, source: ESRAB]. • assets (ships, aircraft) for transport tracking and facilitation in support of sea, land, and air surveillance (includes, e.g. automated number plate / container number recognition systems for vehicles / cargo).
Detection of goods, substances, assets and people and incidents	Detection and screening for dangerous/hazardous or illicit goods and substances: • Detection of weapons, explosives, drugs, contraband, Radiation and nuclear materials), including screening of passengers, luggage, cargoes, post and parcels, vehicles etc. • Detection of hidden/concealed persons and substances hidden within persons. • Specialised detection for CBRN substances and agents. Detection of vehicle movements, personnel, abnormal behaviour and other potential threats in specific environments (e.g. marine / maritime, air, land/rail border, critical infrastructures, public spaces, crowds, etc.); • Detection of large and small fast boats, underwater vehicles, swimmers in ports and harbours and wider maritime environment; • Detection of manned and unmanned vehicles, e.g. UAVs, light aircraft • Detection of people trying to enter [the EU territory] illegally • Intruder detection / illicit access to buildings (detection of unwanted entities in close proximity to critical infrastructures) • Detection of abnormal behaviour patterns of individuals or groups of individuals (terrorist, criminal behaviour) • Detection of abnormal behaviour patterns of vehicles and goods (in terms of their trajectory on the outside of critical infrastructures).

High Level Security Functions	Description
	• Intruder detection / illicit access to buildings (detection of unwanted entities in close proximity to critical infrastructures) • Detection of water contamination • Remote detection of illicit access to pipelines • Detection of people and contaminated environments in case of a crisis or security incident. Includes, inter alia: • Detection of people (wounded, injured, buried alive, etc.) • Detection of ill and/or infectious persons • Detection of contaminated environments • Detection of contaminants in supply networks (e.g. water system contamination) Detection of security / crisis incidents for early warning (e.g. Incident detection systems for fire, gas leaks, smoke alarms, etc.)
Positioning and localisation, tracking and tracing	Positioning, localisation and tracking of platforms, goods, cargo containers, vehicles (including ships, aircraft), people and inventories: • Localisation and tracking of goods, containers and vehicles in an area (e.g. bar codes, applications that secure integrity of cargo containers such as electronic seals with tracking/positioning such as GPS, RFID…) • Tracking of containers and goods in wide open areas • Tracking and tracing of hazardous substances (and components for substances) and devices (e.g. weapons, explosives, CBRN agents such as radioactive materials, hazardous chemicals) • Control of property change of chemicals to preclude misuse [source: ESRAB] • Positioning, localisation and tracking of persons (personnel movements), emergency services, inventories and aid relief in crisis situations • Observation and localisation of individuals through sub-terrain, debris, fixed structures (walls, metal, etc.). Includes detection and localisation of victims (wounded, buried alive, etc.) in a crisis incident.
Mobility and deployability	Mobility and deployability of people, assets, equipment for / in: • regular security operations (border management, customs, law enforcement / police patrolling, civil protection, etc.). • security incidents / crisis events (i.e. incident response), including management of resources and distribution logistics.
Investigation and forensics	Tools, forensic equipment and systems, etc. to investigate a security threat event (e.g. to develop 'post event' intelligence to identify perpetrators and collect information for eventual legal proceedings etc., the origin of natural disasters, industrial accidents, etc. (Excluding for digital forensics; see 'Data, information & intelligence gathering management, and exploitation')
Decontamination and neutralisation	Decontamination of ill / contaminated persons and environments (large areas and sites), reagents. Neutralisation of perpetrators and devices (including explosives, CBRN and firearms) and effects of a security / crisis incident:

High Level Security Functions	Description
	• Containment (limitation) of impacts/effects of terrorist device on the environment by isolation shielding material, handcuffs, explosive neutralisation, etc., • Removal of threats (e.g. extinguishers, specialised robots, …), etc., • Restoration and recovery of basic services (e.g. water, communication, energy, etc.), including service/business security (see also cyber – data recovery)
Secure and public communication, data / information exchange	Secure and interoperable communication and information systems for use in • crisis situations (e.g. by police, customs, emergency responders, private security services, etc.), • tactical communications • regular security operations (border surveillance, police patrolling, civil protection operations). Communication equipment and systems for public information management and situation alert (e.g. public information broadcasting, specialised apps, sirens, …)
Training and exercises	Training, virtual reality (VR), emergent reality (ER), workshops, exercises and drills. Includes training platforms and facilities with use of scenario and situation modelling, computer aided training, simulation systems, etc,. Cybersecurity education and training (e.g. on how to use tools, human aspects, security management and governance, trust management and accountability)

4.1.1.1.1.1.3 FCT Taxonomy – Technology Dimension

Technology area L1	Definition	Technology area L2
Access control/authorisation (building access, system access, etc.)	Access control systems ensure that access to assets [or places] is authorised and restricted or limited to identified and verified persons or vehicles only, based on business and security requirements. Authentication systems provide assurance that a claimed characteristic of an entity is correct.	Access control/authorisation (building access, system access, etc.)
		Identification and authentication of persons
		Identification and authentication of documents and objects
Alarm/warning systems	System to detect and indicate the presence of a [person/object/element] or occurrence of an event [disaster/emergency situation] to an alarm zone and giving signals for	Alarm/warning systems
		Alarm/warning systems
		(Perimeter) Intrusion detection/alarm systems
		Other uses

Technology area L1	Definition	Technology area L2
	appropriate action, including alarms/ warning systems for disasters/ natural hazards.	
Data analytics	Data analytics is used to understand objects represented by data (3.1.5), to make predictions for a given situation, and to recommend on steps to achieve objectives. The insights obtained from analytics are used for various purposes such as decision-making, research, sustainable development, design, planning, etc	Data analytics
CBRNE detection and neutralisation products	Tools/products/technology with the ability to detect the presence or use of chemical, biological, radiological, nuclear and explosive (CBRNE) materials at points of manufacture, transportation, and use	CBRNE detection and neutralisation products
		Containment equipment (to prevent unintentional exposure to pathogens, toxins)
		Neutralisation/decontamination solutions
		Detection (Radiation survey meters, dosimeters, etc.)
Data storage and exchange	Systems and tools related to the organisation and exchange of data.	Data storage and exchange
Digital forensics	Scientific tasks, techniques, and practices used in the investigation of stored or transmitted binary information or data for legal purposes	Digital forensics
Digital security products and services	Resources and tools used to secure and protect online identity, data, and other digital assets and technologies	Digital security products and services
		Integrated product security functions
		Code/malware detection and analysis
Facilitation systems and secure databases	Services and facilities related to easing/facilitating the process of a traveller from their point of origin to the destination in a secure way.	Facilitation systems and secure databases
General equipment	Equipment used to support the operations of personnel in civil security.	General equipment
		Vehicles (excl. UAVs, only including vehicles which transport people)
		Logistics & utilities
		Energy
Guarding and physical protection (non-human)	Intended to delay, stop, or guide people, or to provide protection against hazards.	Guarding and physical protection (non-human)

Technology area L1	Definition	Technology area L2
Internet-based investigation	Tools and methods used for online investigations	Internet-based investigation
		Online investigation tools
		Online search tools
		OSINT tools
Laboratory equipment for gathering and forensic analysis of samples	Tools and equipment used by scientists who work in a laboratory	Laboratory equipment for gathering and forensic analysis of samples
Healthcare / medical equipment	Equipment used for health and medical diagnosis and treatment following disease or injury	Healthcare / medical equipment
Monitoring tools and services	System/tools that constantly check/survey people, places and objects which may also provide alerts or alarms and collect data for evaluation	Monitoring tools and services
		Health / Diseases and epidemiological monitoring systems and tools
		Weather/meteorological monitoring systems
		Land/environment/geography
PPE/Safety equipment	Device or appliance designed to be worn or held by an individual for protection against one or more health and safety hazards	PPE/Safety equipment
		Protective clothing (protective garments, protective footwear, hand protection)
		Protective equipment (head, face, eye, respiratory)
		Physiological monitoring
Screening & detection	Tools and devices used to screen and detect risks and threats related to people or objects	Screening & detection
Search devices and tools	Tools and devices used to search [for] people or objects	Search devices and tools
Specialised management & control systems	Specialised management & control systems	Specialised management & control systems
		Management systems
		Decision support/forecasting
		Operating systems
		Command and control
Surveillance systems	System consisting of (camera/video/sensing) equipment, monitoring and associated equipment for transmission and controlling purposes, which may be necessary for the surveillance of a protected area	Surveillance systems
		Unmanned systems (platforms, vehicles)

Technology area L1	Definition	Technology area L2
Tracking, navigation and guiding systems, equipment and tools	Systems / technologies which enable the collection of geospatial data regarding a specific individual, object or area to determine the exact place of a person or entity. Tracking systems / technologies monitor the physical location of a person or entity; tracking technologies can also be used for determining who was in a geographic area [...] at a particular time". Note: overlaps with surveillance and monitoring.	Tracking, navigation and guiding systems, equipment and tools
Training & Simulation	Tools and services that teach skills or competences.	Training & Simulation
		Training platforms and systems
		Simulation tools
		Thematic training
Conflict management / Use of force	Objects or devices designed or that can be used for inflicting bodily harm or physical damage.	Conflict management / Use of force
		Lethal weapons
		Non-lethal weapons
Critical communications, Interoperable communications	Systems and technologies that ensure the ability to maintain communications, information sharing and diffusion across diverse systems and organisations (public safety actors, emergency / first responders, etc.) and wit the public in any environmental condition. with responders in any environmental conditions.	Critical communications, Interoperable communications
		Communications systems and networks
		Communications devices (radio-based, wireless)

Appendix B. Initial set of data sources

The following table shows the initial list of data sources to be considered by the Observatories during the first implementation cycle. These sources have been characterised according to the attributes defined in section 2.2 of this document. The result of the characterisation is too massive to be included in this document. The full characterisation file is available upon request to the ENACT project coordinator and through the project website.

#	Source of information	Relevant to CapO	Relevant to TechO	Relevant to MktO	Relevant to ELSO	Category
1	CEN/CENELEC Events	LOW	MEDIUM	HIGH	LOW	Event
2	ECSO Events	LOW	MEDIUM	HIGH	LOW	Event
3	ENLETS Events	MEDIUM	HIGH	LOW	LOW	Event
4	DG HOME CERIS NEWS	HIGH	MEDIUM	LOW	MEDIUM	News and media
5	DG HOME RAN NEWS	HIGH	LOW	LOW	MEDIUM	News and media
6	DG HOME NEWS	HIGH	LOW	LOW	MEDIUM	News and media
7	EUROPOL NEWS	HIGH	MEDIUM	LOW	MEDIUM	News and media
8	CEPOL Highlights	HIGH	LOW	LOW	MEDIUM	News and media
9	Research Executive Agency Security NEWS	MEDIUM	HIGH	LOW	LOW	News and media
10	Guardia Civil (SP) NEWS	HIGH	LOW	LOW	LOW	News and media
11	Policia (SP) NEWS	HIGH	LOW	LOW	LOW	News and media
12	Ertzaintza (SP) News	HIGH	LOW	LOW	LOW	News and media
13	Digital security magazine	MEDIUM	HIGH	MEDIUM	LOW	News and media

Funded by the European Union

#	Source of information	Relevant to CapO	Relevant to TechO	Relevant to MktO	Relevant to ELSO	Category
14	ENISA News	HIGH	HIGH	LOW	LOW	News and media
15	El Radar APTIE - News	MEDIUM	HIGH	MEDIUM	LOW	News and media
16	Esmartcity news	MEDIUM	HIGH	MEDIUM	LOW	News and media
17	Euractiv - Technology news	MEDIUM	HIGH	MEDIUM	MEDIUM	News and media
18	HORIZON FCT Active project news[19]	MEDIUM	HIGH	LOW	MEDIUM	News and media
19	Horizon Standardisation Booster News	LOW	MEDIUM	HIGH	LOW	News and media
20	Science business news	LOW	HIGH	MEDIUM	MEDIUM	News and media
21	IFAFRI events	HIGH	HIGH	LOW	LOW	News and media
22	STARLIGHT Project - FCT Project 2020 - News and Multimedia	MEDIUM	MEDIUM	MEDIUM	MEDIUM	News and media
23	EITHOS Project - FCT Project 2021 - News and Events	MEDIUM	MEDIUM	MEDIUM	MEDIUM	News and media
24	MultiRATE Project - SSRI Project 2021 - News	MEDIUM	MEDIUM	MEDIUM	MEDIUM	News and media
25	FALCon Project - FCT Project 2022 - News	MEDIUM	MEDIUM	MEDIUM	MEDIUM	News and media
26	AIDA Project - FCT Project 2019 - News and Events	MEDIUM	MEDIUM	MEDIUM	MEDIUM	News and media
27	DANTE Project - FCT Project 2015 - News	MEDIUM	MEDIUM	MEDIUM	MEDIUM	News and media
28	ANITA Project - FCT Project 2017 - News	MEDIUM	MEDIUM	MEDIUM	MEDIUM	News and media

[19] The list of FCT projects included in Appendix C contains 32 active projects at the date of release of this deliverable. Their websites will be added to the data sources list.

#	Source of information	Relevant to CapO	Relevant to TechO	Relevant to MktO	Relevant to ELSO	Category
29	EACTDA - EUROPEAN ANTI-CYBERCRIME TECHNOLOGY DEVELOPMENT ASSOCIATION - News	MEDIUM	MEDIUM	MEDIUM	MEDIUM	News and media
30	ECTEG - European Cybercrime Training and Education Group - News	MEDIUM	MEDIUM	MEDIUM	MEDIUM	News and media
31	ENFSI - European Network of Forensic Science Institutes - News	MEDIUM	MEDIUM	MEDIUM	MEDIUM	News and media
32	France's Observatory on Scientific and Technological Innovation for Security	HIGH	HIGH	LOW	LOW	News and media
33	TECNOSEC Noticias	MEDIUM	HIGH	HIGH	LOW	News and media
34	SICUR Noticias	MEDIUM	HIGH	HIGH	LOW	News and media
35	USEC Noticias	MEDIUM	HIGH	HIGH	LOW	News and media
36	IDENTITY WEEK EUROPE News	MEDIUM	HIGH	HIGH	LOW	News and media
37	ISO News	LOW	MEDIUM	HIGH	LOW	News and media
38	UNE - Revista de Normalización Española	MEDIUM	MEDIUM	HIGH	LOW	News and media
39	FORENSIC FOCUS - Digital Forensics roundup	LOW	HIGH	HIGH	LOW	News and media
40	NLP Planet	LOW	MEDIUM	LOW	LOW	News and media
41	European Police Congress - News	HIGH	HIGH	MEDIUM	LOW	News and media
42	IPVM - Physical Security Technology Information	LOW	MEDIUM	MEDIUM	LOW	News and media
43	Forensic	LOW	MEDIUM	LOW	LOW	News and media

#	Source of information	Relevant to CapO	Relevant to TechO	Relevant to MktO	Relevant to ELSO	Category
44	Interpol News and Events	HIGH	MEDIUM	LOW	LOW	News and media
45	European IP Helpdesk News	LOW	MEDIUM	HIGH	MEDIUM	News and media
46	IEEE - Electronic Newsletter of the Technical Commitee on Security & Privacy	MEDIUM	HIGH	HIGH	LOW	News and media
47	CEN/CENELEC News	LOW	MEDIUM	HIGH	LOW	News and media
48	ETSI News	LOW	MEDIUM	HIGH	LOW	News and media
49	ECSO News	LOW	MEDIUM	HIGH	LOW	News and media
50	ENLETS News	MEDIUM	HIGH	LOW	LOW	News and media
51	Council of Europe: Cybercrime news	HIGH	MEDIUM	LOW	MEDIUM	News and media
52	ISF National Programme 2021-2027 - SPAIN	HIGH	HIGH	MEDIUM	LOW	Other
53	ISF National Programme 2021-2027 - ITALY	HIGH	HIGH	MEDIUM	LOW	Other
54	EPE - Europol Platform of Experts (limited to LEAs)	HIGH	MEDIUM	LOW	LOW	Other
55	Interpol Innovation Snapshots	HIGH	HIGH	LOW	HIGH	Other
56	Interpol Procurement	MEDIUM	MEDIUM	HIGH	LOW	Other
57	EU Policy on Child Sexual Abuse	HIGH	LOW	LOW	HIGH	Policy papers and updates
58	EU Policy on Corruption	HIGH	LOW	LOW	HIGH	Policy papers and updates
59	EU Policy on Counter Terrorism and Radicalisation	HIGH	LOW	LOW	HIGH	Policy papers and updates
60	EU Policy on Cybercrime	HIGH	LOW	LOW	HIGH	Policy papers and updates
61	EU Policy on Organised Crime and Human Trafficking	HIGH	LOW	LOW	HIGH	Policy papers and updates

#	Source of information	Relevant to CapO	Relevant to TechO	Relevant to MktO	Relevant to ELSO	Category
62	European Parliament research service	HIGH	MEDIUM	LOW	LOW	Policy papers and updates
63	European Parliament legislative train schedule	HIGH	LOW	LOW	MEDIUM	Policy papers and updates
64	Council of the European Union - Home Affairs Updates	HIGH	LOW	LOW	HIGH	Policy papers and updates
65	United Nations - Research on criminal justice	HIGH	LOW	LOW	LOW	Policy papers and updates
66	United Nations - Research on Corruption	HIGH	LOW	LOW	LOW	Policy papers and updates
67	United Nations - Global report on trafficking in persons (2009-2022)	HIGH	LOW	LOW	LOW	Policy papers and updates
68	United Nations - Global study on homicide (2019)	HIGH	LOW	LOW	LOW	Policy papers and updates
69	United Nations - Global study on firearms trafficking (2020)	HIGH	LOW	LOW	LOW	Policy papers and updates
70	United Nations - Data Matters	HIGH	LOW	LOW	LOW	Policy papers and updates
71	United Nations - Evaluation Reports: Countering Transnational Organized Crime	HIGH	LOW	LOW	LOW	Policy papers and updates
72	European Strategy and Policy Analysis System (ESPAS)	MEDIUM	HIGH	LOW	LOW	Policy papers and updates
73	European Union Institute for Security Studies (EUISS)	MEDIUM	MEDIUM	LOW	LOW	Policy papers and updates
74	European Data Protection Supervisor	LOW	LOW	LOW	HIGH	Policy papers and updates
75	ISO Update	LOW	MEDIUM	HIGH	LOW	Policy papers and updates
76	ECSO Publications	LOW	MEDIUM	HIGH	LOW	Policy papers and updates
77	EU Terrorism Situation & Trend Report (TE-SAT)	HIGH	MEDIUM	LOW	MEDIUM	Practitioner reports

#	Source of information	Relevant to CapO	Relevant to TechO	Relevant to MktO	Relevant to ELSO	Category
78	Internet Organised Crime Threat Assessment (IOCTA)	HIGH	HIGH	LOW	MEDIUM	Practitioner reports
79	Serious and Organised Crime Threat Assessment (SOCTA)	HIGH	MEDIUM	LOW	MEDIUM	Practitioner reports
80	DG HOME Publications	HIGH	LOW	LOW	MEDIUM	Practitioner reports
81	Frontex risk analysis	HIGH	MEDIUM	LOW	LOW	Practitioner reports
82	EuCB Innovation Lab - Monthly Reports	MEDIUM	MEDIUM	LOW	HIGH	Practitioner reports
83	GO-Science EmTech Library (need approval by UK GVT)	HIGH	HIGH	MEDIUM	LOW	Practitioner reports
84	European Union Agency of Law Enforcement Training (CEPOL)	MEDIUM	MEDIUM	LOW	HIGH	Practitioner reports
85	European Union Crime Prevention Network	MEDIUM	MEDIUM	LOW	LOW	Practitioner reports
86	Foresight towards the 2nd Strategic Plan for Horizon Europe	LOW	HIGH	LOW	LOW	Practitioner reports
87	EMPACT results factsheets 2022	HIGH	MEDIUM	LOW	LOW	Practitioner reports
88	eu-LISA Industry Roundtable LOOKING AHEAD ENSURING CYBER-RESILIENCE OF EU IT SYSTEMS AGAINST EMERGING THREATS	LOW	MEDIUM	LOW	LOW	Practitioner reports
89	eu-LISA Annual Report	LOW	MEDIUM	LOW	LOW	Practitioner reports
90	EUROJUST Publications	MEDIUM	LOW	LOW	LOW	Practitioner reports
91	UK forensic-science-regulator-newsletters-and-reports	MEDIUM	MEDIUM	MEDIUM	MEDIUM	Practitioner reports
92	ENLETS Reports	MEDIUM	HIGH	LOW	LOW	Practitioner reports

#	Source of information	Relevant to CapO	Relevant to TechO	Relevant to MktO	Relevant to ELSO	Category
93	UNOCD Teaching module series	HIGH	MEDIUM	LOW	LOW	Practitioner reports
94	STARLIGHT Project - FCT Project 2020 - Website results	MEDIUM	MEDIUM	MEDIUM	MEDIUM	Project results
95	DANTE Project - FCT Project 2015 - Results	MEDIUM	MEDIUM	MEDIUM	MEDIUM	Project results
96	ANITA Project - FCT Project 2017 - Results	MEDIUM	MEDIUM	MEDIUM	MEDIUM	Project results
97	ENFSI - European Network of Forensic Science Institutes - Results	MEDIUM	MEDIUM	MEDIUM	MEDIUM	Project results
98	Tender Electronic Daily	LOW	MEDIUM	HIGH	LOW	Public database
99	OLAF calls for tender	MEDIUM	MEDIUM	HIGH	LOW	Public database
100	Union anti-fraud programme Hercule component - Calls for proposals 2023	MEDIUM	MEDIUM	HIGH	LOW	Public database
101	EU Security Market study - Market segmentation model	MEDIUM	MEDIUM	HIGH	LOW	Public database
102	United Nations - Corruption & economic crime (2003-2021)	HIGH	LOW	LOW	LOW	Public database
103	United Nations - Environmental crime (2014 - 2021)	HIGH	LOW	LOW	LOW	Public database
104	United Nations - Intentional crime (1990 - 2022)	HIGH	LOW	LOW	LOW	Public database
105	United Nations - Violent & sexual crime (2003-2021)	HIGH	LOW	LOW	LOW	Public database
106	United Nations - Prisons & Prisoners (1998 - 2023)	HIGH	LOW	LOW	LOW	Public database
107	United Nations - Access & Functioning of Justice (2003-2021)	HIGH	LOW	LOW	LOW	Public database
108	United Nations - Trafficking in Persons (2003-2021)	HIGH	LOW	LOW	LOW	Public database
109	NATO Library Catalog	LOW	LOW	LOW	LOW	Public database
110	Open Security Data Europe	LOW	MEDIUM	MEDIUM	HIGH	Public database
111	Council of Europe Cybercrime Programme Office (EU C-PROC)	MEDIUM	HIGH	LOW	MEDIUM	Public database
112	Horizon Dashboard	LOW	HIGH	HIGH	LOW	Public database
113	Open Repository Base on International Strategic Studies (ORBIS)	LOW	HIGH	LOW	MEDIUM	Scientific Material

Appendix C. Mapping of FCT projects H2020-Horizon Europe to EU Security Taxonomy

The following table shows the list of FCT projects and the topics they are associated with. These projects have been mapped to the EU Security Taxonomy following the analysis carried out in the first ENACT Analytical Report. The result of the mapping is too massive to be included in this document. The file is available is available upon request to the ENACT project coordinator and through the project website.

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
2PS	2PS - Prevent & Protect Through Support	101073949	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101073949	2410865,5	2410866,25	24	HORIZON-RIA	HORIZON-CL3-2021-FCT-01-11
TRACE	Tracking illicit money flows	101022004	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/101022004	6980082,5	7115082,5	18	RIA	SU-FCT02-2018-2019-2020
ALADDIN	Advanced hoListic Adverse Drone Detection, Identification Neutralization	740859	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/740859	4998240	5253827,5	20	RIA	SEC-12-FCT-2016-2017
ANITA	Advanced tools for fighting oNline Illegal TrAfficking	787061	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/787061	4999580	5131767,5	18	RIA	SEC-12-FCT-2016-2017

Funded by the European Union

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
TITANIUM	Tools for the Investigation of Transactions in Underground Markets	740558	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/740558	4991600	5042670	16	RIA	SEC-12-FCT-2016-2017
Ceasefire	Advanced versatile artificiaAdvanced versatile artificial intelligence technologies and interconnected cross-sectoral fully-operational national focal points for combating illicit firearms trafficking	101073876	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101073876	4999808,75	6227583,17	24	HORIZON-IA	HORIZON-CL3-2021-FCT-01-10
ARIES	reliAble euRopean Identity EcoSystem	700085	H2020-EU.3.7.	https://cordis.europa.eu/project/id/700085	2247002,5	2379971,25	11	RIA	FCT-09-2015

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
ASGARD	Analysis System for Gathered Raw Data	700381	H2020-EU.3.7.	https://cordis.europa.eu/project/id/700381	11992553,25	12062954,7	36	RIA	FCT-01-2015
AUGGMED	Automated Serious Game Scenario Generator for Mixed Reality Training	653590	H2020-EU.3.7.	https://cordis.europa.eu/project/id/653590	5535673,75	5535673,75	15	RIA	FCT-07-2014
CC-DRIVER	Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour	883543	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/883543	4997630	5066692,5	14	RIA	SU-FCT01-2018-2019-2020
CCI	Cutting Crime Impact – Practice-based innovation in preventing,	787100	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/787100	3095068,75	3095068,75	12	RIA	SEC-07-FCT-2016-2017

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	investigating and mitigating high-impact petty crime								
EXFILES	Extract Forensic Information for LEAs from Encrypted SmartPhones	883156	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/883156	6999596,25	7084283,75	15	RIA	SU-FCT02-2018-2019-2020
City.Risks	Avoiding and mitigating safety risks in urban environments	653747	H2020-EU.3.7.	https://cordis.europa.eu/project/id/653747	3934811	3934811	14	RIA	FCT-10-2014
CITYCoP	Citizen Interaction Technologies Yield Community Policing	653811	H2020-EU.3.7.	https://cordis.europa.eu/project/id/653811	5576716	5576716,25	24	RIA	FCT-14-2014
CLARUS	Building clarity and preventing bias in digital forensic	101121182	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101121182	2180563,94	2180563,94	12	HORIZON-RIA	HORIZON-CL3-2022-FCT-01-02

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	examination, interorganisational communication and interaction								
ARIEN	ARtificial IntelligencE in fighting illicit drugs production and traffickiNg	101121329	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101121329	4268160	4944397,5	18	HORIZON-IA	HORIZON-CL3-2022-FCT-01-06
RAMSES	Internet Forensic platform for tracking the money flow of financially-motivated malware	700326	H2020-EU.3.7.	https://cordis.europa.eu/project/id/700326	3532000	3955181,86	14	IA	FCT-04-2015
CounteR	Privacy-First Situational Awareness Platform for Violent Terrorism and Crime Prediction,	101021607	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/101021607	6994812,5	7132312,5	21	RIA	SU-FCT02-2018-2019-2020

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	Counter Radicalisation and Citizen Protection								
CREST	Fighting Crime and TerroRism with an IoT-enabled Autonomous Platform based on an Ecosystem of Advanced IntelligEnce, Operations, and InveStigation Technologies	833464	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/833464	6999078,75	6999078,75	25	RIA	SU-FCT02-2018-2019-2020
DANTE	Detecting and ANalysing TErrorist-related online contents and	700367	H2020-EU.3.7.	https://cordis.europa.eu/project/id/700367	4998527,88	6283903,75	20	IA	FCT-06-2015

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	financing activities								
DARLENE	Deep AR Law Enforcement Ecosystem	883297	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/883297	6954860	7337735	17	RIA	SU-FCT02-2018-2019-2020
EITHOS	European Identity THeft Observatory System	101073928	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101073928	2996141,25	2996141,25	12	HORIZON-RIA	HORIZON-CL3-2021-FCT-01-12
EMERITUS	Environmental crimes' intelligence and investigation protocol based on multiple data sources	101073874	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101073874	4634193,75	5929437,5	23	HORIZON-IA	HORIZON-CL3-2021-FCT-01-09
ENTRAP	Enhanced Neutralisation of explosive Threats Reaching Across the Plot	740560	H2020-EU.3.7.,H2020-EU.3.7.2.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/740560	4978248,75	5063583,75	17	RIA	SEC-11-FCT-2016

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
HEROES	Novel Strategies to Fight Child Sexual Exploitation and Human Trafficking Crimes and Protect their Victims	101021801	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/101021801	4999500	5587230	29	RIA	SU-FCT01-2018-2019-2020
FALCON	Fight Against Large-scale Corruption and Organised Crime Networks	101121281	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101121281	4720938	5124835	26	HORIZON-IA	HORIZON-CL3-2022-FCT-01-05
FERMI	Fake nEws Risk MItigator	101073980	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101073980	3999815	4467965	17	HORIZON-IA	HORIZON-CL3-2021-FCT-01-03
FORENSOR	FOREnsic evidence gathering autonomous seNSOR	653355	H2020-EU.3.7.	https://cordis.europa.eu/project/id/653355	4043546,25	4937833,94	11	IA	FCT-05-2014
IcARUS	Innovative AppRoach	882749	H2020-EU.3.7.,H2020-	https://cordis.europa.eu/project/id/882749	5291015,74	5326265,74	20	RIA	SU-FCT01

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	to Urban Security		EU.3.7.1.,H2020-EU.3.7.8.						-2018-2019-2020
GATHERINGS	COMMON STANDARDS FOR SECURITY, PRIVACY AND COST OF THE SURVEILLANCE OF PUBLIC GATHERINGS	101121200	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101121200	2826716,25	3039140,36	11	HORIZON-CSA	HORIZON-CL3-2022-FCT-01-04
GEMS	Gaming Ecosystem as a Multilayered Security Threat	101121345	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101121345	2864352,5	2864352,5	10	HORIZON-RIA	HORIZON-CL3-2022-FCT-01-03
PROACTIVE	PReparedness against CBRNE threats through cOmmon Approaches between security praCTItioners and the	832981	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/832981	4970028,75	4970028,75	16	RIA	SU-FCT01-2018-2019-2020

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	VulnerablE civil society								
RAYUELA	EMPOWERING AND EDUCATING YOUNG PEOPLE FOR THE INTERNET BY PLAYING	882828	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/882828	4974290	4978040	17	RIA	SU-FCT01-2018-2019-2020
SHOTPROS	SHOTPROS: A HUMAN FACTORS BASED (VR) TRAINING FRAMEWORK FOR DECISION-MAKING AND ACTING CAPABILITIES UNDER STRESS AND IN HIGH-RISK SITUATIONS FOR	833672	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/833672	5059843,75	5059843,75	13	RIA	SU-FCT01-2018-2019-2020

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	EUROPEAN LEAS								
ICT4COP	Community-Based Policing and Post-Conflict Police Reform	653909	H2020-EU.3.7.	https://cordis.europa.eu/project/id/653909	4999998	4999999	12	RIA	FCT-14-2014
IMPRODOVA	Improving Frontline Responses to High Impact Domestic Violence	787054	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/787054	2929073,75	2929073,75	17	RIA	SEC-07-FCT-2016-2017
CONNEXIONs	InterCONnected NEXt-Generation Immersive IoT Platform of Crime and Terrorism DetectiON, PredictiON, InvestigatiON, and PreventiON Services	786731	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/786731	4999390	4999390	21	RIA	SEC-12-FCT-2016-2017
INDEED	Strengthening a	101021701	H2020-EU.3.7.,H2020-	https://cordis.europa.eu/project/id/101021701	4983330	4983330	19	RIA	SU-FCT01

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	comprehensive approach to preventing and counteracting radicalisation based on a universal evIdeNce-based moDEl for Evaluation of raDicalisation prevention and mitigation		EU.3.7.1.,H2020-EU.3.7.8.						-2018-2019-2020
INFINITY	IMMERSE. INTERACT. INVESTIGATE	883293	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/883293	6866503,75	7095132,41	23	RIA	SU-FCT02-2018-2019-2020
INHERIT	INHibitors, Explosives and pRecursor InvesTigation	101021330	H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/101021330	4882980	5010742,5	14	IA	SU-FCT04-2020

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
INSPEC2T	Inspiring CitizeNS Participation for Enhanced Community PoliCing AcTions	653749	H2020-EU.3.7.	https://cordis.europa.eu/project/id/653749	4911548,75	4911548,75	18	RIA	FCT-14-2014
COPKIT	Technology, training and knowledge for Early-Warning / Early-Action led policing in fighting Organised Crime and Terrorism	786687	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/786687	4986973,75	5189291,25	20	RIA	SEC-12-FCT-2016-2017
MAGNETO	Multimedia Analysis and Correlation Engine for Organised Crime Prevention and Investigation	786629	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/786629	5320475	5485200	25	RIA	SEC-12-FCT-2016-2017

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
LAGO	LESSEN DATA ACCESS AND GOVERNANCE OBSTACLES	101073951	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101073951	6522673,5	7441298,75	27	HORIZON-IA	HORIZON-CL3-2021-FCT-01-04
LAW-GAME	An Interactive, Collaborative Digital Gamification Approach to Effective Experiential Training and Prediction of Criminal Actions	101021714	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/101021714	6999490	6999490	22	RIA	SU-FCT02-2018-2019-2020
LAW-TRAIN	Mixed-reality environment for training teams in joint investigative interrogation-Intelligent interrogatio	653587	H2020-EU.3.7.	https://cordis.europa.eu/project/id/653587	5095687	5095687,5	11	RIA	FCT-07-2014

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	n training simulator								
LETS-CROWD	Law Enforcement agencies human factor methods and Toolkit for the Security and protection of CROWDs in mass gatherings	740466	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/740466	2919307,5	2979307,5	19	RIA	SEC-07-FCT-2016-2017
RED-Alert	Real-time Early Detection and Alert System for Online Terrorist Content based on Natural Language Processing, Social Network Analysis,	740688	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/740688	5064437,5	5114437,5	19	RIA	SEC-12-FCT-2016-2017

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	Artificial Intelligence and Complex Event Processing								
SPIRIT	Scalable privacy preserving intelligence analysis for resolving identities	786993	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/786993	4998656,25	4998656,25	18	RIA	SEC-12-FCT-2016-2017
MARGIN	Tackle Insecurity in Marginalized Areas	653004	H2020-EU.3.7.	https://cordis.europa.eu/project/id/653004	1881399,5	1881399,5	7	CSA	FCT-13-2014
MEDIA4SEC	The emerging role of new social media in enhancing public security	700281	H2020-EU.3.7.	https://cordis.europa.eu/project/id/700281	1902006,25	1917006,25	10	CSA	FCT-15-2015
microMole	SEWAGE MONITORING SYSTEM FOR TRACKING SYNTHETI	653626	H2020-EU.3.7.	https://cordis.europa.eu/project/id/653626	4992866,33	5423798,5	11	IA	FCT-05-2014

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	C DRUG LABORATORIES								
MINDb4ACT	Mapping, IdentifyiNg and Developing skills and opportunities in operating environments to co-create innovative, ethical and effective ACTions to tackle radicalization leading to violent extremism	740543	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/740543	2999309,5	2999309,5	18	RIA	SEC-06-FCT-2016
NOSY	New Operational Sensing sYstem	653839	H2020-EU.3.7.	https://cordis.europa.eu/project/id/653839	4198684,63	5442257,68	15	IA	FCT-05-2014
ODYSSEUS	PREVENTING, COUNTERING, AND INVESTIGA	101021857	H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/101021857	4996350	5604543,75	18	IA	SU-FCT04-2020

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	TING TERRORIST ATTACKS THROUGH PROGNOSTIC, DETECTION, AND FORENSIC MECHANISMS FOR EXPLOSIVE PRECURSORS								
Pericles	Policy recommendation and improved communication tools for law enforcement and security agencies preventing violent radicalisation	740773	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/740773	2999647,5	2999647,5	15	RIA	SEC-06-FCT-2016

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
PERIVALLON	Protecting the EuRopean terrItory from organised enVironmentAl crime through inteLLigent threat detectiON tools	101073952	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101073952	4670653,75	5379572,5	24	HORIZON-IA	HORIZON-CL3-2021-FCT-01-09
POLIIICE	Powerful Lawful Interception, Investigation, and Intelligence	101073795	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101073795	4202787,5	4383038,5	24	HORIZON-RIA	HORIZON-CL3-2021-FCT-01-02
PRACTICIES	Partnership against violent radicalization in the cities	740072	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/740072	3378970	3424782,5	28	RIA	SEC-06-FCT-2016
VICTORIA	Video analysis for Investigation of Criminal and	740754	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/740754	5007125	5678596,83	19	RIA	SEC-12-FCT-2016-2017

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	TerrORIst Activities								
AIDA	Artificial Intelligence and advanced Data Analytics for Law Enforcement Agencies	883596	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/883596	7690272,5	8853485	21	IA	SU-FCT03-2018-2019-2020
PROPHETS	Preventing Radicalisation Online through the Proliferation of Harmonised ToolkitS	786894	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/786894	2998331,25	2998331,25	15	RIA	SEC-07-FCT-2016-2017
PROTAX	New Methods to PRevent, Investigate and Mitigate COrruption and TAX Crimes in the EU	787098	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/787098	2992633,75	2992633,75	9	RIA	SEC-07-FCT-2016-2017
PROTON	Modelling the PRocesses leading to	699824	H2020-EU.3.7.	https://cordis.europa.eu/project/id/699824	4094811,5	4464506,68	21	RIA	FCT-16-2015

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	Organised crime and TerrOrist Networks								
APPRAISE	fAcilitating Public & Private secuRity operAtors to mitigate terrorIsm Scenarios against soft targEts	101021981	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/101021981	7999101,25	9448081,75	29	IA	SU-FCT03-2018-2019-2020
FORMOBILE	From mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices	832800	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/832800	6983030	6983030	19	RIA	SU-FCT02-2018-2019-2020
GRACE	Global Response Against Child Exploitation	883341	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/883341	6823512,5	6906387,5	23	RIA	SU-FCT02-2018-2019-2020
RISEN	Real-tIme on-site	883116	H2020-EU.3.7.,H2020-	https://cordis.europa.eu/project/id/883116	6995876,25	7069876,25	21	RIA	SU-FCT02

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	forenSic tracE qualificatio N		EU.3.7.1.,H2020-EU.3.7.8.						-2018-2019-2020
RITHMS	Research, Intelligence and Technology for Heritage and Market Security	101073932	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101073932	4996972,5	5056972,5	20	HORIZON-RIA	HORIZON-CL3-2021-FCT-01-08
ROCSAFE	Remotely Operated CBRNe Scene Assessment Forensic Examination	700264	H2020-EU.3.7.	https://cordis.europa.eu/project/id/700264	4781061,25	4781061,25	13	RIA	FCT-03-2015
ROXANNE	Real time network, text, and speaker analytics for combating organized crime	833635	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/833635	6999458,75	6999458,75	26	RIA	SU-FCT02-2018-2019-2020
IMPROVE	Improving Access to Services for Victims of Domestic	101074010	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101074010	2978095,5	3185790	16	HORIZON-IA	HORIZON-CL3-2021-

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	Violence by Accelerating Change in Frontline Responder Organisations								FCT-01-06
INSPECTr	Intelligence Network and Secure Platform for Evidence Correlation and Transfer (INSPECTr)	833276	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/833276	6997910	7101035	21	RIA	SU-FCT02-2018-2019-2020
SHUTTLE	Scientific High-throughput and Unified Toolkit for Trace analysis by forensic Laboratories in Europe	786913	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.7.	https://cordis.europa.eu/project/id/786913	9511053,77	11050232,5	9	PCP	SEC-09-FCT-2017
ISEDA	Innovative Solutions to Eliminate Domestic Abuse	101073922	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101073922	2678523,88	2947827,5	15	HORIZON-IA	HORIZON-CL3-2021-FCT-01-06

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
SYSTEM	SYnergy of integrated Sensors and Technologies for urban sEcured environMent	787128	H2020-EU.3.7.,H2020-EU.3.7.2.,H2020-EU.3.7.1.,H2020-EU.3.7.7.	https://cordis.europa.eu/project/id/787128	7926171,45	9090790,35	24	IA	SEC-10-FCT-2017
TAKEDOWN	Understand the Dimensions of Organised Crime and Terrorist Networks for Developing Effective and Efficient Security Solutions for First-line-practitioners and Professionals	700688	H2020-EU.3.7.	https://cordis.europa.eu/project/id/700688	3146375	3421062,5	20	RIA	FCT-16-2015

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
TARGET	Training Augmented Reality Generalised Environment Toolkit	653350	H2020-EU.3.7.	https://cordis.europa.eu/project/id/653350	5992359,75	5992360	18	RIA	FCT-07-2014
TENACITY	Travelling Intelligence Against Crime and Terrorism	101074048	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101074048	4439136,25	5538186,25	19	HORIZON-IA	HORIZON-CL3-2021-FCT-01-01
TENSOR	Retrieval and Analysis of Heterogeneous Online Content for Terrorist Activity Recognition	700024	H2020-EU.3.7.	https://cordis.europa.eu/project/id/700024	4562975	5979100	21	HORIZON-IA	FCT-06-2015
TENSOR	Reliable biomeTrictEhNologies to asSist Police authorities in cOmbating terrorism and	101073920	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101073920	4977200,5	5763198,35	19	IA	HORIZON-CL3-2021-FCT-01-05

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	oRganized crime								
LOCARD	Lawful evidence collecting and continuity platform development	832735	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/832735	6833385	6983862,5	23	RIA	SU-FCT02-2018-2019-2020
PREVISION	Prediction and Visual Intelligence for Security Information	833115	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/833115	8001180	9320792,5	33	IA	SU-FCT03-2018-2019-2020
TRILLION	TRusted, CItizen - LEA coILaboratIon over sOcial Networks	653256	H2020-EU.3.7.	https://cordis.europa.eu/project/id/653256	4263407,5	4263407,5	20	RIA	FCT-14-2014
TRIVALENT	Terrorism pReventIon Via rAdicaLisation countEr-NarraTive	740934	H2020-EU.3.7.6.,H2020-EU.3.7.,H2020-EU.3.7.1.	https://cordis.europa.eu/project/id/740934	2720420	2720420	21	RIA	SEC-06-FCT-2016
UNCOVER	Development of an efficient steganalysi	101021687	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.8.	https://cordis.europa.eu/project/id/101021687	6929517,5	7034389,81	24	RIA	SU-FCT02-2018-

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
	s framework for uncovering hidden data in digital media.								2019-2020
Unity	Unity	653729	H2020-EU.3.7.	https://cordis.europa.eu/project/id/653729	4330900	4538120	16	RIA	FCT-14-2014
SAFE-CITIES	riSk-based Approach For the protEction of public spaces in European CITIES	101073945	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101073945	2752617,5	3342123,75	19	HORIZON-IA	HORIZON-CL3-2021-FCT-01-07
VANGUARD	adVANced technoloGical solutions coupled with societal-oriented Understanding and AwaReness for Disrupting trafficking in human beings	101121282	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101121282	4536682,5	4862445	23	HORIZON-IA	HORIZON-CL3-2022-FCT-01-07

Project acronym	Title	ID	Programmes	URL	Net EU Contribution	Total Cost	Participation	Type of Action	TOPIC
VIGILANT	Vital IntelliGence to Investigate ILlegAl DisiNformation	101073921	HORIZON.2.3.2,HORIZON.2.3	https://cordis.europa.eu/project/id/101073921	3376604,5	3905630	19	HORIZON-IA	HORIZON-CL3-2021-FCT-01-03
VISAGE	Visible Attributes through Genomics: Broadened Forensic Use of DNA for Constructing Composite Sketches from Traces	740580	H2020-EU.3.7.,H2020-EU.3.7.1.,H2020-EU.3.7.7.	https://cordis.europa.eu/project/id/740580	5000000	5007778,75	13	RIA	SEC-08-FCT-2016

Appendix D. ENACT Memorandum of Understanding

In line with the Networking Strategy, as part of the Networking tools, and in order to facilitate the collaboration with other projects, entities and experts, ENACT will seek to establish a number of Memoranda of Understanding (according to KPI1.1.5). To that extent, the following template is provided as reference under this deliverable. The template will be updated accordingly on a case-by-case basis taking into account the nature of the collaboration to be established.

MEMORANDUM OF UNDERSTANDING

BETWEEN:

XXX – ……[insert name of the Project] (Grant Agreement No ……..) represented by …….. [insert name of the Representative] of ……..[insert name of the Party], XXX Project Coordinator,

YYY – ……[insert name of the Project] (Grant agreement No…….), represented by ……..[insert name of the Representative] of ……..[insert name of the Party], YYY Project Coordinator,

Parties hereby agree as follows:

ARTICLE 1: Scope

The purpose of the MoU is to set up the preliminary terms of understanding between the parties to facilitate the negotiations, on a more detailed cooperation scheme, between the Parties, subject to the terms and conditions detailed hereunder. It is expressly understood and agreed that the provisions of this MoU only constitute the indication of the Parties' common interest to cooperate with each other regarding the subject as described hereunder. Except for the obligations expressly laid down herein, i.e., the Duty of Non-Disclosure of Article 3, nothing contained in this MoU shall be construed as binding nor as compelling either Party to enter into any contractual relationship. No Party may claim any indemnity from the other Party/Parties should the Parties fail to reach an agreement on the contemplated cooperation.

ARTICLE 2: Motivation of collaboration

Opportunities for synergies and cooperation have been identified in the following fields:

1. Joint dissemination activities and public events:

Funded by the European Union

- Each project/entity will share logo, description and relevant news of the other project/entity on its website.
- Share invitation to workshops and relevant events, including public demonstrations.
- Co-organisation of workshops

2. Stakeholder engagement:
   - ENACT Observatorium knowledge sharing
   - …….
   -
3. Validation activities:
   - ……
   - ……..
4. Exploitation activities:
   - ……..
   - ……

ARTICLE 3: Duty of Non-Disclosure

THE PARTIES HERETO AGREE AS FOLLOWS:

1. Confidential Information

1.1 For the purposes of this Agreement, Confidential Information means any data or information that is proprietary to or possessed by a Party and not generally known to the public or that has not yet been revealed, whether in tangible or intangible form, whenever and however disclosed, including, but not limited to:

(i) any scientific or technical information, invention, design, process, procedure, formula, improvement, technology or method;

(ii) any concepts, samples, reports, data, know-how, works-in-progress, designs, drawings, photographs, development tools, specifications, software programs, source code, object code, flow charts, and databases;

(iii) any marketing strategies, plans, financial information, or projections, operations, sales estimates, business plans and performance results relating to the Party's past, present or future business activities, or those of its affiliates, subsidiaries and affiliated companies and organisations;

(iv) trade secrets; plans for products or services, and customer or supplier lists;

(v) any other information that should reasonably be recognised as Confidential Information by the Parties.

1.2 The Parties agree hereby that Confidential Information needs not to be novel, unique, patentable, copyrightable or constitute a trade secret to be designated Confidential Information and therefore protected.

1.3 Confidential Information shall be identified either by marking it, in the case of written materials, or, in the case of information disclosed orally or written materials that are not marked, by notifying the other Party of the confidential nature of the information. Such

notification shall be done orally, by e-mail or written correspondence, or via other appropriate means of communication.

1.4 The Parties hereby acknowledge that the Confidential Information proprietary to each Party has been developed and obtained through great efforts and shall be regarded and kept as Confidential Information.

1.5 For the purposes of this Agreement, the Party which discloses Confidential Information within the terms established hereunder to the other Party shall be regarded as the Disclosing Party. Likewise, the Party which receives the disclosed Confidential Information shall be regarded as the Receiving Party.

1.6 Notwithstanding the aforementioned, Confidential Information shall exclude information that:

(i) is already in the public domain at the time of disclosure by the Disclosing Party to the Receiving Party or thereafter enters the public domain without any breach of the terms of this Agreement;

(ii) was already known by the Receiving Party before the moment of disclosure (under evidence of reasonable proof or written record of such disclosure);

(iii) is subsequently communicated to the Receiving Party without any obligation of confidence from a third party who is in lawful possession thereof and under no obligation of confidence to the Disclosing Party;

(iv) becomes publicly available by other means than a breach of the confidentiality obligations by the Receiving Party (not through fault or failure to act by the Receiving Party);

(v) is or has been developed independently by employees, consultants or agents of the Receiving Party (proved by reasonable means) without violation of the terms of this Agreement or reference or access to any Confidential Information pertaining to the Parties.

2. Purpose of the Disclosure of Confidential Information

The Parties will enter into collaboration searching for opportunities for synergies and mutual cooperation, as defined above in this MoU, in the following fields:

1. Organisation/Co-organisation of joint dissemination activities and public events;
2. Stakeholder Engagement;
3. ……
4. ……..

3. Undertakings of the Parties

3.1 In the context of discussions, the Disclosing Party may disclose Confidential Information to the Receiving Party. The Receiving Party agrees to use the Confidential Information solely in connection with purposes contemplated between the Parties in this Agreement, and not to use it for any other purpose or without the prior written consent of the Disclosing Party.

3.2 The Receiving Party will not disclose and will keep the information received confidential, except to its employees, representatives or agents who need to have access to the Confidential Information to carry out their duties in connection with the permitted purposes specified in clause 2. The Receiving Party will inform them about the confidential quality of the information provided and will ensure that their agreement is obtained to keep it confidential, on the same terms as set forth in this Agreement. Hence the Receiving Party will be responsible for ensuring that the obligations of confidentiality and non-use contained herein will be strictly observed, and will assume full liability for the acts or omissions made for its personnel representatives or agents.

3.3 The Receiving Party will use the Confidential Information exclusively for the permitted purpose stated in clause 2 and not use it for its own purposes or benefit.

3.4 The Receiving Party will not disclose any Confidential Information received to any third parties, except as otherwise provided for herein.

3.5 The Parties shall treat all Confidential Information with the same degree of care as it accords to its own Confidential Information.

3.6 All Confidential Information disclosed under this Agreement shall be and remain the property of the Disclosing Party and nothing contained in this Agreement shall be construed as granting or conferring any rights to such Confidential Information on the other Party. Principally, nothing in this Agreement shall be deemed to grant to the Receiving Party a licence expressly or by implication under any patent, copyright or other intellectual property right. The Receiving Party acknowledges and confirms that all existing and future intellectual property rights related to the Confidential Information are exclusive titles of the Disclosing Party. For the sake of clarity based on reciprocity and good faith of the Parties, the Receiving Party will not apply for or obtain any intellectual property protection regarding the Confidential Information received. Likewise, any modifications and improvements by the Receiving Party shall be the sole property of the Disclosing Party.

3.7 The Receiving Party shall promptly return or destroy all copies (in whatever form reproduced or stored), including all notes and derivatives of the Confidential Information disclosed under this Agreement, upon the earlier of (i) the completion or termination of the dealings contemplated in this Agreement; (ii) or the termination of this Agreement; (iii) or at the time the Disclosing Party may request it to the Receiving Party.

3.8 Notwithstanding the foregoing, the Receiving Party may retain such documents as required to comply with mandatory law, provided that such Confidential Information or copies thereof shall be subject to an indefinite confidentiality obligation.

3.9 In the event that the Receiving Party is asked to communicate the Confidential Information to any judicial, administrative, regulatory authority or similar or obliged to reveal such information by mandatory law, it shall promptly notify the Disclosing Party of the terms of such disclosure, and will collaborate to the extent practicable with the Disclosing Party to comply with the order and preserve the confidentiality of the Confidential Information.

3.10 The Parties agree that the Disclosing Party will suffer irreparable damage if its Confidential Information is made public, released to a third party, or otherwise disclosed in breach of this Agreement; and that the Disclosing Party shall be entitled to obtain injunctive

relief against a threatened breach or continuation of any such breach and, in the event of such a breach, an award of actual and exemplary damages from any court of competent jurisdiction.

3.11 The Receiving Party shall immediately notify the Disclosing Party upon becoming aware of any breach of confidence by anybody to whom it has disclosed the Confidential Information and give all necessary assistance in connection with any steps which the Disclosing Party may wish to take to prevent, stop or obtain compensation for such a breach or threatened breach.

3.12 The Confidential Information subject to this Agreement is made available "as such" and no warranties of any kind are granted or implied with respect to the quality of such information including, but not limited to, its applicability for any purpose, non-infringement of third-party rights, accuracy, completeness or correctness.

3.13 Neither Party is under any obligation under this Agreement to disclose any Confidential Information it chooses not to disclose. Further, neither Party shall have any liability to the other Party resulting from any use of the Confidential Information except with respect to disclosure of such Confidential Information in violation of this Agreement.

3.14 Nothing in this Agreement shall be construed to constitute an agency, partnership, joint venture, or other similar relationship between the Parties.

ARTICLE 4. Duration and Miscellaneous

1 Duration and Termination

Except as expressly modified herein, all terms and conditions of the Agreement shall remain unchanged and in full force and effect.

Notwithstanding the foregoing, the Receiving Party's duty to hold in confidence Confidential Information that was disclosed during the term shall remain in effect indefinitely, save otherwise agreed.

2 Applicable Law and Jurisdiction

This Agreement shall be construed and interpreted by the …… law. The court of ……. shall have jurisdiction.

3 Liability

With the exception of direct damages caused by a Party's wilful misconduct or gross negligence, neither Party will be held liable by the other Party/Parties for any direct or indirect, incidental or consequential damages of such Party/Parties or any third party resulting from the present MoU. A Party's aggregate liability towards the other Parties collectively shall be limited to once the Party's share of the total costs of the Project in which the liable Party participates.

4 Validity

If any provisions of this Agreement are invalid or unenforceable, the validity of the remaining provisions shall not be affected. The Parties shall replace the invalid or unenforceable

provision by a valid and enforceable provision, that will meet the purpose of the invalid or unenforceable provision as closely as possible.

5 Subsequent Agreements

Ancillary agreements, amendments or additions hereto shall be made in writing.

6 Costs

Each Party shall bear its own costs, fees or other expenses incurred during the term and

in connection with the MoU. No financial compensation whatsoever shall be due by either Party to the other Party(ies) under the MoU

7 Communications

Any notices or communications required between the Parties shall be delivered by hand, e-mail, or mailed by registered mail to the address of the other Party as indicated below. Any subsequent modification of a Party's address should be reasonably communicated in advance to the effect of this Agreement.

FOR [insert name of the Party]

Email: [insert email address]
Postal address: [insert address]

FOR [insert name of the Party]

Email: [insert email address]
Postal address: [insert address]

ARTICLE 5. Competition

The receipt of Confidential Information and Datasets pursuant to this Agreement will not prevent or in any way limit either Party from developing, making or marketing products or services that are or may be competitive with the products or services of the other; or providing products or services to others who compete with the other Party; as long as those results have not become from a breach of this Agreement.

……
……

IN WITNESS WHEREOF, the Parties hereto have caused this MoU to be executed as of the date stated below.

FOR XXXXX [insert name of the Party] [insert name of representative]

[insert title]
Done at [place] on [date]

FOR YYYYY [insert name of the Party] [insert name of representative]

[insert title]
Done at [place] on [date]

Appendix E. Detailed Task Workplan Template

1. TX.Y description and objectives

TX.Y aims to… <description, more concrete than the DoA >
The task receives information from:

- …

The task provides information to:

- ...

1. Task objectives

Concrete and, *as much as possible*, **measurable goals.**

Title		**ID**	**TO-X.Y-01**
Description		**Contributing sub-task(s)**	TX.Y.1, TX.Y.2
Type	*	**Related to tasks**	TY.J, TX.Z
Rationale			
Internal Milestones			
Success Criteria			
Comments			
Last update			

….
** Type list to be determined in final DTW template version. Can be more than one. Can choose from: policy, tech, standards, R&I (project results), research, networking, CDE, cooperation.*

2. Sub-tasks

1. TX.Y.1 Title

Description:
Expected results:

- …
- …

Table 1. TX.Y.1 Planned Partner Effort

Partner	Contribution	Planned effort (PMs)
A	Contribution 1	*
	Contribution 2	
B	…	

..	..	
…	…	…

[Planned effort is not carved in stone nor has to be the final effort reported. Purpose is to ensure understanding among contributors about the analogies of work per contributor, i.e. partner A will do minor work on this sub-task, partner B none at all, partner C will focus heavily on this sub-task, partner D will distribute their efforts among 3 sub-tasks, etc.]

2. TX.Y.2 Title

…

3. Request for contributions

Contributions required by other project tasks. Task leader to inform relevant partners or ensure their discussions upon circulation of final version of the DTW.

Table 2. Task Request for Contributions

Task	Partners	Contribution
TY.W	…	Provide …

4. Risks / Issues

Table 3. Identified Task Risks/issues

Risk/Issue	Description

5. Contribution to deliverable(s)

This task will contribute to deliverable(s) DX.X, … .