



## ILEAnet

Innovation by Law Enforcement Agencies networking

### **Deliverable 5.17:**

### **Public report on the ILEAnet findings n°9**

Grant Agreement number: 740714	H2020-SEC-2016-2017-1
Start date of project: 1 June 2017	Duration: 60 months
Lead beneficiary of this deliverable: ENSP	Deliverable type: Report
Dissemination Level : Public	Release: V1
Due date of deliverable: 31/01/2022	Actual submission date: 31/01/2022
Description: Based on contributions from WP1-WP4, the public report summarises the main results from ILEAnet: practitioner challenges and needs, recommendations for uptake of RDI results, best practice exchange, standardisation, future RDI activities.	



# INNOVATION BY LAW ENFORCEMENT AGENCIES NETWORKING



## Public Report on ILEAnet findings n°9

### **Description**

Based on contributions from WP1-WP4, public report summarising the main results from ILEAnet: practitioner challenges and needs, recommendations for uptake of RDI results, best practice exchange, standardization, future RDI activities.

## Executive Summary

This public report aims to give an insight to the work performed within ILEAnet from month 49 to 54 (June – November 2021).

The ILEAnet Community has continued to live and grow. In November 2021, the community counted more than 280 members connected through the ILEAnet online platform, but their participation goes beyond their digital activities. A daily work is undertaken by the Community Management team to reinforce and boost the ILEAnet practitioners' and researchers' community. Given the global sanitary situation, ILEAnet's goal to build an online community of practitioners and researchers had more incidence.

One of the great accomplishments under the reporting period has been the exploration of the standardisation topic. Two specific activities have been carried out: the in-depth analysis of the areas of most common interest for future standardisation and the roll out of a Public Workshop dedicated to *Standardisation in security research* (hereafter referred to as PW4, see chapter about WP4 for further information).

The ILEAnet Project Uptake Process (IPUP), a qualitative process designed to support the uptake of existing innovative solutions, has been further explored thanks to a webinar held in collaboration with FOLDOUT and iProcureNet projects. Based on its previous experience with the ROBORDER IPUP webinar, ILEAnet has adapted its tools (such as the post webinar questionnaire) to explore the next steps for the solution uptake (see chapters about WP3 and WP4).

A continuous work is done to better involve practitioners in security research. It is ILEAnet's core mission to connect researchers and law enforcement practitioners through joint events (e.g. workshops) but also research-focused activities, such as in-depth studies.

During the reporting period, the two subcontracted studies have moved forward (see chapter about WP5 and WP6 for further information). The first one, which started in April 2021, studies *Information sharing mechanisms between European Law Enforcement Agencies*. The first two tasks have been completed and the team is now working on the final stage, which is the drafting of recommendations, based on the study's findings. The second study on *Age Determination assessment techniques* has been awarded and moved very fast, with two tasks completed. The team is now working on classifying the identified techniques in order of relevance and for different use cases. Both studies have performed states of the start and explored potential solutions to either a cross-cutting (Information Sharing) or a specific (Age determination) need identified by the ILEAnet community. These studies will feed WP2.

The scientific coordination team has continued to propose a set of offers to researchers, in order to reinforce the connections among them and with practitioners. The INCs have fully taken over the scientific newsletter to disseminate information about practitioners-researchers and their activities in security research areas. The INCs have also actively participated in enlarging the ILEAnet community by inviting researchers and other law enforcement practitioners (see chapter about WP1).

In order to perpetuate its main findings, ILEAnet worked on defining and unfolding its sustainability plan, especially regarding the Knowledge Factory (see chapter about WP3). This work will be speed up in the coming weeks and the project team will design its final event (the ILEAnet Public Workshop 5) in that perspective.

As a wrap-up work, WP2 initiated a broad analysis activity, aiming at comparing the LEAs' challenges and needs analysed during the

course of the project, with current issues faced by practitioners.

A detailed description of the activities performed in each of the three technical WPs is provided in this report, and structured as follows:

- Report of the general activities
- Strategy for the next six months

Furthermore, an additional section presents the crosscutting activities, not necessarily visible in the three technical work packages, but nonetheless crucial for the success of the project.

## Table of content

Executive Summary .....	3
Introduction.....	6
The ILEAnet project .....	6
The ILEAnet Workflow: “the cycle” .....	8
The ILEAnet Online Platform .....	9
Main findings .....	10
WP1: ILEAnet networking, including INC role and contribution to topic strands.....	10
The ILEAnet National Contacts (INCs) .....	10
Report of general activities .....	11
Strategy for the next six months .....	12
WP2 Law Enforcement Challenges and Needs.....	13
Report of general activities .....	13
Strategy for the next six months .....	15
WP3 ILEAnet Knowledge Factory .....	16
Report of general activities .....	16
Strategy for the next six months .....	17
WP4 ILEAnet Scouting activities.....	18
Report of general activities .....	18
Strategy for the next six months .....	21
WP5 and WP6: transversal activities.....	22
Conclusion .....	23
Annex 1 – Results of WP4 on areas requiring further standardisation.....	25
Annex 2 - Guidelines for research projects invited to present their work during ILEAnet Public Workshop 4 on standardisation .....	26

# Introduction

## The ILEAnet project

ILEAnet is a European project funded by the European Union's Horizon 2020 research and innovation programme and launched on the 1st of June 2017 for a 5-year duration. The overall objective of ILEAnet is to build and develop a sustainable organizational Law Enforcement Agency (LEA) practitioners' network focused on Research, Development and Innovation (RDI). ILEAnet addresses LEA challenges, together with a community of individuals, including practitioners and experts from academia and industry, interesting in exchanging and collaborating in this area.

Detailed information about the project is available online ([www.ileanet.eu](http://www.ileanet.eu)).

The ILEAnet Network and Community were created adopting a two-way perspective: top-down and bottom-up.

### ● Top-down:

ILEAnet functions as a network of organisations. It is aligned with existing institutional structures respecting the corresponding institutional mandates and operational set-ups.

### ● Bottom-up:

In addition, ILEAnet functions as a community of people who are interested in innovation-centred collaboration. Thereby, innovation is facilitated, and key LEA challenges are addressed.

The effective iterative interaction between these two approaches helps to identify needs and opportunities and prioritise suggestions with respect to future LEA-relevant RDI in the EU and national programmes, policies and standardisation efforts.



Figure 1: ILEAnet involved countries

21 partners from 17 countries are involved in the project. Most of them are practitioners, together with research centers and institutes (see the table below).

Organisation	Country
Federal Ministry of the Interior	<b>Austria</b>
Ministry of Interior – Bulgaria	<b>Bulgaria</b>
Cyprus Police	<b>Cyprus</b>
Police of the Czech Republic	<b>Czech Republic</b>
Estonian Police and Border Guard Board	<b>Estonia</b>
ARTTIC	<b>France</b>
French Ministry of Interior	<b>France</b>
Ecole Nationale Supérieure de la Police	<b>France</b>
Bavarian University of Applied Sciences for Public Service, Department of Policing (in replacement of the Deutsche Hochschule der Polizei) <sup>1</sup> : <b>to be validated in the amendment under review</b>	<b>Germany</b>
Hungarian National police	<b>Hungary</b>
University College Dublin, Centre for Cybersecurity & Cybercrime Investigation	<b>Ireland</b>
Ministry of Public Security	<b>Israel</b>
Italian Public Safety Department, Ministry of Interior	<b>Italy</b>
State Police of Latvia	<b>Latvia</b>
European Forensic Initiatives Centre	<b>Poland</b>
Police Academy in Szczytno	<b>Poland</b>
Romanian Ministry of Internal Affairs	<b>Romania</b>
Slovakian Criminal Police, Ministry of Interior	<b>Slovakia</b>
ISEMI INSTITUTE	<b>Slovakia</b>
Unitad Central Intelligencia Criminal	<b>Spain</b>
Police Service of Northern Ireland	<b>United Kingdom</b>

Figure 2: ILEAnet Consortium

<sup>1</sup> The organisation signed a non-disclosure agreement and its application to become an ILEAnet organisation member was included in the second amendment to the Grant Agreement submitted to the European Commission in July 2021.

## The ILEAnet Workflow: “the cycle”

As laid out in the Description of the Action (DoA), ILEAnet workflow was to be implemented in annual cycles and articulated around three work packages, based on a close cooperation between inter-related work packages (WP2, WP3 and WP4). This cycle enables ILEAnet to:

1. Define practitioners’ challenges and needs
2. Monitor, collect and organise the current state of the art and existing or recent research initiatives
3. Identify gaps, requirements, opportunities and priorities
4. Provide recommendations and feed them back to the Consortium.



Figure 3: ILEAnet Cycle

It should be noted that the other work packages support the ILEAnet cycle, through the ILEAnet National Contacts and scientific referents’ networks, the project management and scientific coordination, as well as numerous dissemination and communication activities.

## The ILEAnet Online Platform

A collaborative space, encouraging discussions between European LEAs and researchers was created at the beginning of the project. The ILEAnet Online Platform, hosted in the Community Management Tool (CMT), allows an exchange between ILEAnet contributors. The ILEAnet Online Platform is structured with respect to the main topics raised by European practitioners. The interactions are monitored by several members of the ILEAnet team.

The ILEAnet Online Platform is continuously adjusted to the needs of the ILEAnet members.

During the reporting period, a special attention has been paid to easing the navigation in the platform. For instance, the landing page has been simplified (see Figure 4 below) and forum groups, which were no longer active, were closed.

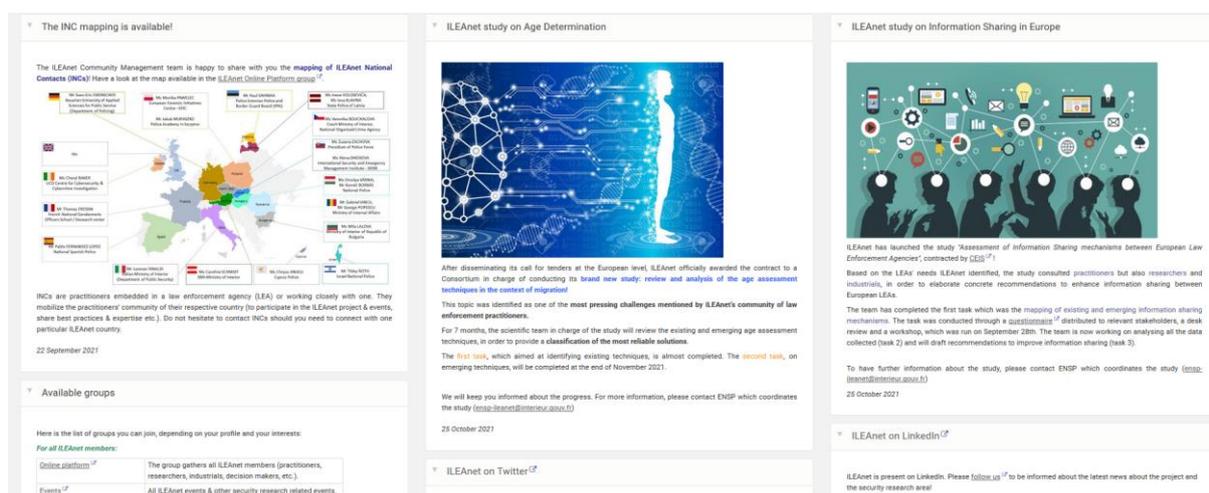


Figure 4: ILEAnet Online Platform Landing page (screenshot of 07 December 2021)

## Main findings

### WP1: ILEAnet networking, including INC role and contribution to topic strands

WP1 aims at providing the resources and inputs from the ILEAnet National Contacts (INCs) and their respective national networks of practitioners, academia, industry and other stakeholders.

#### The ILEAnet National Contacts (INCs)

As a reminder, ILEAnet is organised around ILEAnet National Contacts (INCs), who are

dedicated ILEAnet consortium members or Law Enforcement Agency (LEA) representatives from all involved member states. They are responsible for the functioning of their “national networks”. Together with the Scientific Coordination and the Community Management teams, they ensure good quality of the online exchanges. They act as a hub for the ILEAnet bottom-up and top-down oriented activities.

Organisation	Country	INC
BMI- Ministry of the Interior	Austria	Caroline Schmidt
Ministry of Interior – Bulgaria	Bulgaria	Mila Lalova
Cyprus Police	Cyprus	Chryso Angeli
Police of the Czech Republic	Czech Republic	Veronika Bouchalova
Estonian Police and Border Guard Board	Estonia	Raul Savimaa Hannes Jarvine
French Ministry of Interior	France	Thomas Fressin
<b>To be validated in the amendment in preparation:</b> Bavarian University of Applied Sciences for Public Service, Department of Policing (in replacement of the Deutsche Hochschule der Polizei) <sup>2</sup>	Germany	Sven-Eric Fikenscher Holger Nitsch
Hungarian National police	Hungary	Kornel Borbas Orsolya Varnai
University College Dublin, Centre for Cybersecurity & Cybercrime Investigation	Ireland	Cheryl Baker
Italian Public Safety Department, Ministry of Interior	Italy	Elisabetta Ialongo Lorenzo Rinaldi
Israel National Police -Ministry of Public Security	Israel	Tibby Roth
Latvian State Police	Latvia	Inese Voloseviča Ieva Klavina

<sup>2</sup> The organisation signed a non-disclosure agreement and its application to become an ILEAnet organisation member was included in the second amendment to the Grant Agreement submitted to the European Commission in July 2021.

European Forensic Initiatives Centre Foundation - EFIC	Poland	Monika Pawelec
Institute for Research and Development of the Police Academy in Szczytno	Poland	Jakub Muraszko
Romanian Ministry of Internal Affairs	Romania	Gabriel Iancu George Popescu
Presidium of Police Force	Slovakia	Zuzana Zachova
ISEMI INSTITUTE	Slovakia	Alena Diksova
Spanish National Police	Spain	Pablo Fernández López
Police Service of Northern Ireland	United Kingdom	<i>Under discussion</i>

## Report of general activities

INCs have three main missions within ILEAnet:

- Coordination of the ILEAnet national networks in their respective countries
- Facilitation of the contributions from the national networks to ILEAnet
- Expert contributions to ILEAnet.

The WP1 activities for this six-month period can be summarised as follows:

INCs went on raising awareness about ILEAnet activities nationally. Some INCs were significantly active in promoting the project, such as the Polish INC, who connected ILEAnet with several Polish academics and law enforcement practitioners. The Italian INC benefited from ILEAnet events to connect with new partners and actively worked on enlarging its national law enforcement network.

The INCs have fully appropriated the scientific newsletter to share research-related news and projects with their European counterparts. The Italian and Czech INCs are a good example of this! As a reminder, ILEAnet offers the possibility to promote the work of researchers and practitioners having a researcher hat (see chapter about WP6).

The INCs' role was significant to enlarge the audience for the fourth ILEAnet Public Workshop, as they invited national counterparts and experts to participate in the discussions.

The INCs also contributed to inviting practitioners and researchers to the IPUP webinar run with FOLDOUT (see chapter about WP3) and to the workshop carried out in the frame of the *Information Sharing* subcontracted study (see chapter about WP6). The ILEAnet team warmly thanks the Latvian INCs who were able to propose a keynote speaker for the above mentioned workshop.

The INCs function not only as facilitators of their national networks but also as experts participating in discussions themselves, asking questions, sharing knowledge and interacting with the members in the ILEAnet Online Platform. Some INCs took the time to participate in the online platform and shared news about the EU security research agenda.

Similarly to the previous reporting periods, interactions between INCs and the ILEAnet team were supported by monthly teleconferences and the ILEAnet Coordination team offered interviews to new members to

welcome them in the project and facilitate their integration.

In addition, ILEAnet amplified INCs' networking opportunities (e.g., proposals of cooperation & collaboration for future research projects were offered to Estonian, French, German and Czech INCs).

And finally, yet importantly, INCs were surveyed by WP3 about their use of the Knowledge Factory, with the underlying idea of preparing the sustainability of this ILEAnet tool (see dedicated WP3 chapter below).

### Strategy for the next six months

Once again, the last months have shown how INCs play a key role in building and enlarging the network. Their effort will focus on increasing the number of members by enhancing the involvement of the national practitioners and researchers.

INCs will continue circulating information about ILEAnet activities and events in their respective countries and contribute to the Knowledge Factory thanks to information received from their respective networks.

Finally, the INCs will play a huge role in preparing ILEAnet final months and will be involved in the reflection about the project sustainability and the final public event (Public Workshop 5 – PW5).

## WP2 Law Enforcement Challenges and Needs

WP2 aims to collect challenges and needs from Law Enforcement Agencies at the national and EU level, in order to facilitate solutions to these issues through research and development activities. The outputs from WP2 feed the WP3, by determining which angle to use to identify best practices and potential subjects for an in-depth analysis.

WP2 is designed to collect and analyse the needs and challenges of LEA practitioners. The data collection is performed using three approaches:

- Top-down, by suggesting topics based on analysis of policy, strategic documents and strategic research agendas,
- Bottom-up, by collecting inputs in open surveys and non-directed interviews,
- Analysis of surveys and observation of the activities within the ILEAnet network.

### Report of general activities

*Trend analysis of LEAs challenges and needs, in comparison to WP2 previous analyses and surveys*

During the reporting period, as starting a new full ILEAnet research cycle would have been truncated by the end of the ILEAnet project, WP2 focused on preparing the analysis and survey that will research the trends in LEA challenges and needs. The objective is to summarise the previously analysed LEAs challenges & needs and present their dynamics & trends. The initial analysis has been outlined by WP2 and is summarized hereafter.

#### • Trends in migration

The pressure for migration to the EU has remained in recent years, even if migration flows dropped in 2020 to its lowest level since

2003, due to the COVID-19 pandemic. Asylum seeking is still at a high level, despite a massive drop, with most asylum seekers coming from Venezuela, Afghanistan and Syria.

The COVID-19 pandemic drove migration policy changes in 2020. Travel restrictions, border closure and restrictions explain the drop in permanent immigrant flows, but Germany remained the main destination country for migrants in 2020.

Non-legal routes and actions are often still used to reach the EU. Besides the continuous routes across the Mediterranean to Southern Europe, new routes emerged, for example from Iraq via Byelorussia to the EU border in Poland and Lithuania. These results indicate that ensuring physical security and safety at the border may still be relevant for EU countries.

COVID-19 did not make illegally mediated migration activities disappear and migrants from some countries of origin (such as Afghanistan) are more likely to face human smuggling.

Illegal border crossings into the EU were slightly reduced in 2020 comparing with 2019, but both the long-term drivers of migration and the short- to medium-term effects of the COVID-19 pandemic may increase migration pressure. Finally, the additional challenge for LEAs is that it is often difficult to distinguish justified asylum seeking (because of physical danger in the country of origin) from economic migration and emerging potential threats to public safety and security.

#### • Trends in Serious and Organised Crime

Serious and organised crime remains a key threat to the internal security of the EU. Approximately 40% of the criminal networks in

the EU are involved in the trade of illegal drugs. Corruption and the abuse of legal business structures are key features of serious and organised crime in Europe (two thirds of criminals use corruption on a regular basis and more than 80 % of the criminal networks use legal business structures). Violence is a key part in the businesses of criminal networks active in the EU as well. Three future areas where organised crime may have interest to infiltrate were spotted by Europol:

- Digitalisation
- Geopolitical factors
- Green transition.

#### Trend in Cybercrime

Criminal activity in cybercrime has increased in recent years, and the pandemic has brought new criminal opportunities.

Ransomwares continue to be a key threat. Criminals use teleworking to scan potential targets' networks for security gaps. Online grooming has increased, benefiting from the increased time spent online by children.

At the same time, cybercriminals develop a more calculated target selection. Personal information and credentials are in high demand for all types of social engineering attacks.

Illegal markets have expanded to different encrypted communication channels due to increased legal action taken by law enforcement. Methods and tools used by cybercriminals are increasingly adopted in other crime areas and the digital criminal ecosystem continues to evolve.

The pandemic has also increased many related online threats: COVID-19 narratives for the online sale of counterfeit medical products, phishing attacks that mimic the emails of health authorities, use of remote working

options or governmental suggestions in order to collect sensitive data from the potential victims, etc.

#### Trends in Terrorism

The number of terrorist attacks is continuously stable in recent years. However, there are some trends that should be taken into account: the number of completed jihadist attacks in Europe in 2020 doubled in comparison with 2019 and all completed jihadist terrorist attacks were carried out by lone actors in most cases using unsophisticated attack methods. The attackers had different background that make prevention more difficult.

Prisons continue to be a place of radicalisation and recruitment by terrorists.

The pandemic did not modify the modus operandi of terrorist behaviours. Restrictions on travel and physical meetings might have led to increased online consumption of terrorist and extremist content and networking.

Based on the analysis, a survey (survey #9 on identifying the trends in challenges and needs of Law Enforcement Agencies in fighting (cyber)crime, terrorism and illegally mediated migration) will be launched in February 2022 and has already been elaborated. The questionnaire will capture the dynamics of LEAs external environment and trends, as well as potential new challenges and needs for LEAs, and compare those results with the initial desk reviews and surveys (ILEAnet Surveys #1 to #8). The final results will be presented in the next WP2 deliverable.

#### *Monitoring of the online discussions*

WP2 continued monitoring the activities and discussions of LEAs on the ILEAnet Online Platform and this activity is ongoing. No new

discussions were raised during the reporting period.

*Connecting with the EU environment to learn and share LEAs needs*

As mentioned in the previous public deliverable, ILEAnet is collaborating with other European RDI projects and EU organisations. In this way, WP2 is working on strengthening the cooperation with iProcureNet (a H2020 project focused on joint procurement). A publicly available summary of LEAs challenges and needs will be presented in the next WP2 deliverable and sent to the iProcureNet team.

In addition, ILEAnet established contacts with Europol Innovation Lab through the involvement of the ILEAnet coordinator (French Ministry of Interior) in the [STARLIGHT](#) project and in the Artificial Intelligence Core Group.

**Strategy for the next six months**

The WP2 team will concentrate on the trend analysis of LEAs' challenges and needs,

comparing it to the initial desk reviews and the 8 ILEAnet Surveys already carried out. The analysis about the trends and potential new challenges and needs for LEAs will be completed and a conclusive survey (the ILEAnet Survey #9) will be conducted to obtain the current opinions of LEAs. Results will be included in the next WP2 deliverable.

In addition, WP2 will devise a publicly available version of the description of WP2 methodology and results.

The WP2 team will participate in the final ILEAnet Public Workshop (PW5) by presenting the methodology for collecting LEAs challenges and needs (identified as one of ILEAnet assets) and outlining respective important findings and results.

Besides those important tasks, WP2 will analyse and feed the relevant information to the ILEAnet Knowledge Factory and continue monitoring the activities and discussions of LEAs on the ILEAnet Online Platform, capturing emerging topics and facilitating the discussions for a smooth networking of LEAs.

## WP3 ILEAnet Knowledge Factory

During the reporting period, WP3 work has been steered by the review meeting the ILEAnet project had with the European Commission in July 2021. Two main activities were thus conducted:

- Development of and reflection on the sustainability of the ILEAnet wiki (the ILEAnet Knowledge Factory)
- Finalisation of the IPUP process

### Report of general activities

#### *Knowledge Factory*

WP3 mostly concentrated on reflecting on the sustainability of the Knowledge Factory as an exploitable asset. As a reminder, the Knowledge Factory is a specific room on the ILEAnet Online Platform encompassing all security-related materials (reports, white papers, national and international research projects, scientific publications, webinar presentations, etc.).

All ILEAnet users are encouraged to contribute to the body of knowledge with their own expertise or experiences, add value and applicability to the information by evaluating knowledge, and search the Knowledge Factory to find ideas, solutions, events, collaboration opportunities in Europe and internationally. In November 2021, there were more than 600 references of information available in the Knowledge Factory, at the disposal of the ILEAnet Community, but despite the encouragement of individuals outside WP3, the tool feeding is only performed by WP3 contributors. In order to continue populating the Knowledge Factory, a 'push' rather than a 'pull' approach was chosen. Relevant entries are published in the ILEAnet scientific newsletter, every 2 months.

During the reporting period, significant preparatory work has been done to support the development of a sustainability plan for the Knowledge Factory.

- WP3 has begun working on consolidating any information held across the ILEAnet Online Platform that is currently not stored in the Knowledge Factory. This will ensure that all relevant and useful information has been captured in one single location.
- INCs were surveyed on the quality and usefulness of the Knowledge Factory. The few responses received showed very positive feedback. The survey showed that the INCs regularly use the Knowledge Factory and share information with their network. However, the 'recommendation' functionality is poorly used. All respondents asserted that the Knowledge Factory should continue as a valuable resource beyond the lifetime of the project. The ILEAnet team will pay a special attention to those results when preparing the exploitation plan of the Knowledge Factory and an infographic presenting the key results of the survey is being designed.

#### *IPUP (ILEAnet Project Uptake Process)*

WP3 further explored the IPUP (ILEAnet Project Uptake Process) initiative thanks to the delivery of a targeted uptake webinar with [FOLDOUT](#). The latter was a research project having received one of the highest levels of feedback following the third Public Workshop (PW3).

To increase the response rate to the webinar survey, the delivery format was slightly changed by including the questionnaire as a live activity.

The webinar, held on 16 September 2021, gathered more than 60 participants, mainly law enforcement representatives interested in border surveillance.

Similarly to the previous IPUP webinar (carried out with [ROBORDER](#)), participants were provided with an information pack prior to the event to allow time for a deeper dive into the solution. The information pack included the original TELOS survey, the scenario and the Project ID card developed for PW3 and the original project presentation.

During the event, the FOLDOUT team succeeded in presenting their solution for border surveillance with many videos and photos, which increased participants' interest. However, and despite the simplicity of the questionnaire (with Yes/No questions), responses to the live survey were low.

The few responses received showed that most respondents assessed that even if the solution was suitable for commercialisation (and their organisations would be interested in purchasing such a technology), the solution

was also suitable for further development and standardisation (the responses were further analysed by WP4, see next chapter). The ILEAnet IPUP webinar opened exploitation opportunities for FOLDOUT thanks to the connection with a broad range of European and international LEAs and with iProcureNet representatives, who delivered a short presentation about procurement that may help exploring exploitation opportunities.

### Strategy for the next six months

During this reporting period, WP3 prepared the ground for the sustainability of the ILEAnet project by collecting valuable feedback from INCs on the Knowledge Factory and running an additional IPUP cycle from end to end.

The following months will be dedicated to the consolidation of the ILEAnet Knowledge Factory and the development of exploitation plans for the IPUP and the Knowledge Factory, which are identified as two ILEAnet assets.

## WP4 ILEAnet Scouting activities

During this reporting period, WP4 has been mainly concerned with its standardisation mission, but has also been involved in the fine-tuning of IPIP and IPUP processes and the two in-depth subcontracted studies.

### Report of general activities

#### *Standardisation*

Most of WP4's work for the reporting period was dedicated to the completion of the fourth ILEAnet Public Workshop (PW4), dedicated to *Standardisation in security research*, and to the analysis of the event's outputs. As mentioned in the previous public report, prior to the workshop, WP4:

- had been involved in the preparation and design of this online event, and
- led a survey with the ILEAnet LEA community to identify areas requiring further standardisation in several domains (terrorism, cybercrime, serious & organised crime and illegal migration, and a 5<sup>th</sup> category related to the involvement of LEAs in Research, Development and Innovation – RDI – projects).

WP4 made sure to dedicate several PW4 sessions to present and discuss the ILEAnet work on standardisation.

First of all, a dynamic session was designed on Day 1 of the PW4 to present to and prioritise with the participants the areas for further standardisation in the 4 ILEAnet domains (terrorism, cybercrime, serious & organised crime and illegal migration). This session was entitled: *“Standardisation domains in security: reflecting on the findings and analysis from ILEAnet studies and identifying priority domains”*. After a description of the methodology and a presentation of the proposals for each domain, participants were

invited to interactively rank the ILEAnet identified areas based on the level of urgency and the level of importance. The results are presented in Annex 1.

After the Public Workshop 4, WP4 conducted a broad analysis to compare the areas suggested by LEAs with the existing EU standards. WP4 also investigated the H2020 Secure Societies calls to spot any projects developing standards related to the ILEAnet proposals. The whole work conducted to identify areas requiring standardisation was compiled, presented and summarised in a final report titled 'Law Enforcement Agencies priorities as regards domains requiring more standardisation', which has been submitted in November 2021 to the European Commission. This report will be a strong basis to draft the final ILEAnet recommendations.

The second PW4 presentation moderated by WP4 took place on Day 3 under the session *“Promoting and improving security practitioners' involvement in RDI: what role for standards?”* and was entitled *“Towards standards: reflecting on findings and results from the ILEAnet study on ways to promote and improve security practitioners' involvement in Research & Innovation”*. After ILEAnet Scientific Facilitator (ENSP) shared the ILEAnet brainstorming results, WP4 presented LEAs' standards proposals in Research, Development and Innovation, obtained via the previously mentioned survey. Indeed, the ILEAnet LEA community was surveyed to see if they had any ideas of standards, which would improve their participation in RDI projects. The results of the consultation were presented and openly discussed with the participants of the Public Workshop 4 (incl. ILEAnet members, LEA representatives, the external experts on standardisation from CEN-CENELEC Technical Committees and other structural initiatives).

That part of the survey will be analysed and summarised in a future WP4 report, and together with PW4 outputs collected during the 3-day event. As a result, WP4's work on recommendation will be fed with very valuable inputs from the public workshop.

#### *Development of ILEAnet external contacts*

Thanks to the ILEAnet Public Workshop on standardisation, WP4 connected with several standardisation stakeholders during the reporting period:

- Philippe Quevauviller, from the European Commission
- Patricia Compard, Chairperson of the CEN/TC 391 Societal and Citizen Security
- Michel Smithuis, Chairperson of the CEN/TC 419 Forensic Science Processes
- Pertti Woitsch, Chairman of the CEN-CENELEC Sector Forum on Security
- Karl Grün, Director of Standardisation at Austrian Standards International.

Among the 11 short-listed RDI projects identified as potential speakers, 5 accepted ILEAnet invite and presented the standardisation work carried out by their research projects:

- [INSPECTr](#)
- [FORMOBILE](#)
- [EUCISE2020](#)
- [DRIVER+](#), and
- [STAIR4SECURITY](#).

They provided interesting inputs for the LEA and research communities on how to carry out standardisation activities in a research project and what the things to do/not to do.

Those 5 projects were requested to answer specific questions prepared by WP4 during their presentations (see Annex 2). It made them present their standardisation activities in

a comprehensive and detailed way, and was very useful for a non-specialised audience.

Besides the PW4, WP4 monitored the progress of other security research initiatives, through CERIS events and workshops organised by other EU research projects.

#### *IPUP (ILEAnet Project Uptake Process)*

As mentioned in the previous chapter, the FOLDOUT project was a subject for the ILEAnet Project Uptake Webinar dedicated to the uptake of the project's results. The IPUP process ended with the post-webinar questionnaire, submitted to webinar's participants to get a clear understanding of the uptake potential of presented solutions. Already used for ROBORDER IPUP webinar (see previous public report), the post-webinar questionnaire was used again for FOLDOUT IPUP webinar after small rearrangements (see WP3 chapter for further details). Three main questions were asked:

1. Do you think that the solution presented by the project is suitable for further development?
2. Do you think the solution is suitable for commercialisation?
3. In your opinion, would the LEA community benefit from standardisation of the solution?

18 respondents out of 65 participants gave their responses. Most respondents represented Law Enforcement Agencies, either as practitioners or employees (civil servants). All respondents said that the solution was suitable for further development and standardisation activities. 63% of respondents claimed their interest to take part in further development. 83% of respondents thought that the FOLDOUT solution was worth being commercialized in the future and 67% of them were interested in using the solution.

The closing questionnaire is the last point in the IPUP process performed by ILEAnet. Having the post-webinar questionnaire as an online set of questions asked during the webinar, with amended questions, showed a better level of response as compared to the one used during the ROBORDER IPUP webinar. Together with the TELOS questionnaire, it is a useful and practical tool to assess project outputs by LEAs.

#### *IPIP (ILEAnet Project Intake Process)*

As explained above, the ILEAnet LEAs representatives were asked what standards they could propose in order to improve their participation in RDI projects, streamline performance of these projects, as well as the use of their final results in practice. A total of 34 proposals were made, which were then grouped into six categories:

- Administration and Support
- Project Management
- Project Initiation
- Project execution
- Dissemination
- Exploitation
- Commercialisation.

This approach is the ILEAnet's response to one of the key tasks set for the “Pan European Networks of practitioners and other actors in the field of security” in the call H2020-SEC-2016-2017-1 Horizon 2020 Secure Societies programme, that ILEAnet participated in: “Practitioners (end-users) in the same discipline and from across Europe can get together to: (...) express common requirements as regards innovations that could fill in capability and other gaps and improve their performance in the future.”

Those responses were publicly presented at and discussed during the ILEAnet Public Workshop 4, in the session entitled “*Promoting and improving security practitioners’ involvement in RDI: what role for standards?*”

*Towards standards: reflecting on findings and results from the ILEAnet study on ways to promote and improve security practitioners’ involvement in Research & Innovation*”. The report on this study will be published in the next reporting period.

#### *Participation in subcontracting activities*

WP4 has continued to dedicate a significant portion of time to monitor the execution of the two awarded studies, namely ‘*Development of mechanisms for better information sharing among law enforcement agencies*’ and ‘*Review and classification of the existing and emerging age assessment techniques in the context of migration*’.

WP4 has actively participated in the follow up meetings, providing valuable insights regarding the usefulness and feasibility of the results in the scope of LEAs perspective.

The two in-depth subcontracted studies have both reached the two thirds of their completions and the remaining work will be the drafting of the final reports, including the recommendations from the studies. Similarly to the previous reporting period, WP4 ensured that the requirements regarding priority standardisation domains were taken into account in the analyses and the team advised on the format of recommendations produced by the two studies.

#### *Recommendations*

As ILEAnet is entering its last stage, there were also intensive discussions about the format and content of the WP4 final deliverables and the recommendations. WP4 finally agreed on the “shape” and “content” of the final conclusions, including the production of recommendations and RDI roadmaps. recommendations will be built on:

- the results of the Information Sharing and Age determination studies,
- standardisation priority areas,
- cross-cutting topics such as how LEAs should be involved in a research project (IPIP), how the research outputs can be taken up by LEAs (IPUP), and how security stakeholders should be involved in standardisation activities.

The task leader is now compiling the results achieved in the previous WP tasks and in other work packages, in order to draft recommendations in the coming weeks.

### Strategy for the next six months

In the next reporting period, WP4 activities will be focused on different tasks:

- Continuing analysing PW4 results & conducting follow up activities
- Monitoring the development of recommendations and standardisation needs from the two subcontracted in-depth studies
- Developing, consulting and finalising the ILEAnet recommendations and roadmaps.

## WP5 and WP6: transversal activities

This chapter sheds a particular light on the transversal activities led within the ILEAnet project during the reporting period.

- The first mission being to build a network of practitioners and researchers, the community management is a crucial part of the project and requires a daily investment from the Community Management.
- The ILEAnet Online Platform is continuously enhanced and updated to facilitate the navigation and find relevant information more easily. The landing page has been simplified and forum groups, which were no longer active, have been closed.
- ILEAnet continued to strengthen its network thanks to bilateral interviews with its new INC members.
- The Scientific coordination team (ENSP) continued to act as a bridge between the Law Enforcement and the research communities. The most tangible example of this work is the progress of two open calls. One of ILEAnet's partners, namely ENSP, is the contracting authority, and has launched two calls on the European and French procurement platforms, to lead in-depth studies on two topics considered as important for the ILEAnet community: the *'Development of mechanisms for better information sharing among law enforcement agencies'* and a *'Review and classification of the existing and emerging age assessment techniques in the context of migration'*. The two studies aim at making researchers work on practitioners' needs and connect these two worlds. For the first tender, on information sharing, the team has completed the two first tasks which were the mapping of existing and emerging information sharing mechanisms and the analysis of such information. The third and last task is the drafting of recommendations. The second tender, on age determination, has been awarded end

of June 2021 and moved very fast. The contractor has already identified existing and emerging age determination techniques and will start classifying them according to ILEAnet parameters (accuracy, speed, ease of use...). Alongside to WP4, ENSP closely monitors the progress of those in-depth studies and is responsible for the administrative follow up.

- The Scientific coordination team continues to offer a set of digital services to attract researchers and foster exchanges between researchers and practitioners, thanks to the promotion of scientific work through the ILEAnet scientific newsletter (5 issues having been released since the activity has been launched).
- The Scientific coordination team also makes sure to feed the Knowledge Factory with scientific publications related to the ILEAnet priority topics (terrorism, organised crime, illegal migration and cybercrime).
- The support team is also involved in the creation of graphical materials (infographics, flyers, etc.). The pictorial aspect of the project tools is key to explain at a glance the tools and methodologies ILEAnet developed and circulating the results of key ILEAnet studies.
- To internally and externally communicate about the project's activities, the ILEAnet newsletter describes the latest news in the project and enables ILEAnet members to stay updated about the project.

Beyond these daily activities, ILEAnet is now working on defining the assets developed in the course of the project and will ensure to keep them going after the end of the project, by collaborating with other EU security research stakeholders (the European Commission, the EU Agencies such as Europol, the other networks of practitioners, etc.).

## Conclusion

ILEAnet's first mission is to build and develop a sustainable LEA practitioners' network focused on research and innovation addressing LEAs' challenges together with a community of individuals. The ultimate goal is to develop a conducive environment for innovation and facilitate practitioners' involvement into research activities and to enhance ILEAnet's legacy among academics and LEA end-users.

During the reporting period, ILEAnet focused its efforts on:

- **Standardisation**, with the completion of the fourth ILEAnet Public Workshop (PW4) on 'standardisation in security research' and the consolidation and drafting of WP4's final report regarding areas for future standardisation
- The roll out of the **ILEAnet Project Uptake Process (IPUP)** with FOLDOUT and the adjustment of the post-webinar questionnaire, a tool to better capture information from LEAs and other security stakeholders about the possible uptake routes
- The fine-tuning of **IPIP (ILEAnet Project Intake Process)** with additional LEA proposals regarding standards, which would make LEAs more involved in research, development and innovation (RDI) projects
- The **trend analysis regarding LEAs challenges and needs**, in order to put into perspective, the challenges and needs identified and analysed during the course of the project
- The **two in-depth subcontracted studies** launched by ILEAnet on needs identified by the LEA community, namely *Information Sharing* and *Age determination*
- The **reinforcement of the collaboration between ILEAnet and academia**, with the

promotion of the work of European security researchers in the scientific newsletter. The latter has been well taken over by INCs, who – like the whole ILEAnet network – are invited to suggest content for the newsletter and particularly to highlight the scientific work carried out in their respective countries

- The **involvement of the INCs, scientific referents and their national networks in ILEAnet** (in particular via the scientific activities such as the scientific newsletter and the two subcontracted studies)
- The collection of inputs from all WPs to draft ILEAnet final **recommendations**
- The **sustainability of ILEAnet assets**. Indeed, ILEAnet has actively started to prepare its final months and a special work has been conducted in the framework of WP3 on the **ILEAnet Knowledge Factory**, which encompasses all security-related materials generated by the ILEAnet project and community. The INC community was surveyed to assess the level of use of the tool, with very positive and promising feedbacks.

Looking ahead, ILEAnet next months will be focused on:

- Fostering the collaboration between LEAs and academics, taking advantage of ILEAnet events, in-depth studies but also promotion of the scientific work through ILEAnet communication channels
- Encouraging the INC network to feed the platform with RDI activities and make their national network grow continuously
- Drawing the main trends regarding LEAs challenges and needs
- Completing the subcontracted studies
- Drafting and circulating the final recommendations

- Communicating about the main ILEAnet findings (public reports, policy briefs, infographics, scientific publications, etc.)
- Preparing the final ILEAnet event
- Connecting with other key European security stakeholders to strengthen the legacy of ILEAnet tools
- Rolling out the sustainability plan for ILEAnet assets.

Feel free to contact your [national INC](#) and/or your [scientific referent](#) to join the ILEAnet Community!

# Annex 1 – Results of WP4 on areas requiring further standardisation

<b>LEAST</b>  <b>MOST</b>				
<b>MIGRATION</b>				
<b>IMPORTANT</b>				
Human age assessment	Automated linguistic translation	Surveillance and border management	Combating migrant smuggling	Information sharing on human trafficking
<b>URGENT</b>				
Automated linguistic translation	Human age assessment	Information sharing on human trafficking	Surveillance and border management	Combating migrant smuggling
<b>CYBERCRIME</b>				
<b>IMPORTANT</b>				
Economic cybercrime	Crimes on-line (ex aequo)	Response (ex aequo)	Safeguarding privacy	Prevention
<b>URGENT</b>				
Economic cybercrime	Safeguarding privacy (ex aequo)	Response (ex aequo)	Surveillance and border management	Prevention
<b>SERIOUS &amp; ORGANISED CRIME</b>				
<b>IMPORTANT</b>				
Crimes against cultural goods	Environmental crimes	Information sharing on OCG activities	Prevention	Warning systems
<b>URGENT</b>				
Crimes against cultural goods	Environmental crimes	Information sharing on OCG activities	Prevention	Warning systems
<b>TERRORISM</b>				
<b>IMPORTANT</b>				
Intelligence on terrorist recruitment	Information sharing on terrorist activities	Prevention (ex aequo)	Terminology (ex aequo)	Warning systems
<b>URGENT</b>				
Terminology	Intelligence on terrorist recruitment	Prevention	Information sharing on terrorist activities	Warning systems
<b>CROSS-CUTTING DOMAINS</b>				
<b>IMPORTANT</b>				
Open-source intelligence	Improving quality of data	International criminal investigations	Evidence exchange	Sharing criminal information
<b>URGENT</b>				
Open-source intelligence	Improving quality of data	International criminal investigations	Evidence exchange	Sharing criminal information

## Annex 2 - Guidelines for research projects invited to present their work during ILEAnet Public Workshop 4 on standardisation

### “Standardisation in security research”

Advice and recommendations for projects' presentations

#### 1. The standardisation framework of your project

- What was the H2020 call you participated in?
- How were the standard/standardisation requirements addressed in the call? Please quote the requirements directly from the H2020 Work Programme and make your comments based on your consortium experience:
  - Was the standardisation requirement, as expressed in the call, clear enough and fully understandable for your consortium?
  - What kind of problems (if any) did your consortium face while elaborating your application to meet the standardisation requirement?
- Were there other initial reasons for addressing standardisation in your project (aside from the call's requirement)?
  - Requirement from the market
  - Requirement from the legislation
  - Critical activity to do, in order to conduct project's research

activities (common terminology/methodology...)

- Critical activity to ensure the success of the exploitation of the project's results or market strategy
- Etc.

#### 2. Your project proposal

- What did you plan to do to fulfil those standardisation requirements in the proposal you submitted to the EC?
- Briefly describe the project's concrete objectives and elaborate on the standardisation approach you planned to achieve. For instance, you proposed to:
  - Use existing standards for the research activities
  - Conduct research activities on standardisation aspects
  - Develop and revise new standards
  - Draft technical requirements or specification for future standards
  - Participate in standardisation workshops or committees
  - Etc.

#### 3. Your methodology

- What path towards standardisation (methodology) did you choose/ are you choosing/ will you choose in your project?
- Please describe your methodology and the standardisation activities you carried out (or will carry out)
  - What was the general standardisation goal you wanted to achieve?
  - Did you foresee a dedicated Work Package for standardisation aspects or was it spread among other Work Packages?
  - What were the actions you did plan to do towards standardisation?

- Who were the main standardisation actors among your project partners and outside your project (standardisation bodies, professional associations, industry groups...)? How did you choose the standardisation stakeholders and what were the actions (if any) you did foresee for them to do within your project?
- When have the main standardisation activities been implemented in your project? (at the beginning of the project, throughout the project, during the final phase of the project, etc.)

#### 4. Your standardisation results

- In the frame of your project, what are the outcomes of your standardisation efforts?
- Please briefly explain the progress of your work as described in 3. (i. e. the current state-of-play).
- What are the concrete results you have achieved up to now?
- Did the implication of the partner in charge of standardisation impact technological choices in any way? If so, how?
- What are the final standardisation results you plan to achieve at the end of your project? For instance:
  - Harmonised research methodology / standard test procedures
  - Recommendations and/or requirements for new or revised standards
  - Common terminology
  - One of the standardisation tools proposed by the CEN CENELEC
  - A CEN Workshop Agreements (CWAs)
  - Technical Specifications
  - A Technical Report
  - Development of a new standard
  - Etc.

#### 5. Problems

- What kind of problems (if any) did your consortium face on the way towards your standardisation goals?
- Please shortly explain the problems. Examples:
  - Difficulties in prioritizing the standardisation actions within the consortium
  - Misunderstanding of the standardisation goals
  - Difficulties in cooperating with the external standardisation partners (e.g standardisation bodies, LEAs, Universities, Industry, etc.)
  - Lack of commitment from stakeholders
  - Reluctance of some consortium partners in implementing standardisation activities
  - Etc.

#### 6. Feedbacks

- What kind of feedback (if any) have your consortium received as for your standardisation goals and efforts?
  - What was the feedback that you received from the stakeholders about your standardisation goals?
  - How were the standardisation efforts/outcomes assessed by the European Commission auditors?
  - How were your standardisation efforts assessed by the project consortium itself? Was it an easy part of the project for the consortium or the most complicated one?
  - What is your personal assessment of the standardisation part in your project? Was it, in your perception, an important part of your project for the rest of the consortium or marginal?

## 7. Your take-away message

- 🌐 What is the message that you want to share with the other projects working on standardisation and with the LEAs?
- 🌐 To what extent was standardisation important for the success of your project?

Examples:

- Benefits/disadvantages of the standardisation process
- Do's, Don'ts, things to keep in mind, things not to do etc.
- What you retrospectively would have done differently
- Things to improve to facilitate the creation of standards
- Any recommendation, good advice for LEAs

## 8. To be proactive, you'd recommend to work on...

- 🌐 Do you have any suggestions for other topics or areas requiring further standardisation in the EU Security field?

***Please do not exceed 30 minutes and 15 slides of presentation!***

***The objective is to share your project's experience with standardisation, starting from the call to concrete outputs.***