i-LEAD
innovation - law enforcement agency's dialogue

Newsletter
Issue #4 - January 2020

i-LEAD Project
Innovation - Law Enforcement Agency's dialogue
i-LEAD will build the capacity to monitor the security research and technology market in order to ensure a better matching and uptake of innovations by law enforcement agencies with the overarching aim to make it a sustainable Pan-Europan LEA network.

i-LEAD Editorial

Dear all,

I am travelling to Paris where I will meet the Work packages leaders of our project. We will prepare the next review for the European Commission, so its time to reflect and look at our achievements and pitfalls in an honest way.

Basic line, Our project is doing very well and it not only delivers the mandatory documents on time, but there is something bigger, and even more important, the work we are doing is being recognised across Europe.

Our project is mentioned as an example of a well organised ecosystem where law enforcement, industry and academia are coming together. This is an achievement on it's own, because it is the first Lea coordinated H2020 project in this way

So …. why is this project running so well? One of the secrets is the passion and ambition of our work packages leaders but also the engaging work sessions we offer our police colleagues. The feedback is very positive and the question is most "when is the next workshop?" We are taking up and addressing the current challenges from a practitioners view which is appealing, our colleagues want to discuss their daily challenges which connects them strongly.

We have also learned a lot: writing a proposal, emphasising and answering the call text ended up in a successful proposal, but we wrote a very ambitious proposal.

We learned that the outcome of the workshops for our police colleagues delivered so many requirement and needs, that we are unable to scan all relevant technology. We have therefore decided to focus on the key requirements that have been requested by our police colleagues at the workshops.

Whilst the workshops will be still the same, we have decided that the outcome of the workshop will end up in a script, a story telling methodology that summarises a scenario that was defined in the workshop.

Additionally, in the other work package, we will mind map the potential solutions that can add value or relevant research.

This brings a new focus to our work, but also it will drive us to the next step. A better understanding of our needs will mean that we have the opportunity to exploit the results better.

We will also aim to showcase the outcome better; use more graphs, videos and drawings to "paint the picture".

Another lesson we have learnt is that we have phrased the name of our project correctly: a well organised dialogue is needed to bridge between the mindset of a police officers, a representative from academia and / or the industry. We have common goals, but different backgrounds and talents.

We will continue and improve the project day by day. I am already looking forward to the next industry day. At the last industry day a number of companies showcased their solutions and it was very impressive!

We still have a number of challenges ahead however. One of which is the implementation of the front office as "a one stop shop" for those who would like to learn or contribute to the project. This means freeing enough resources and well organised exploitation.

And last but not least; ensuring that other stakeholders will embrace the I-Lead methodology as a best practice and a stepping stone for a modern law enforcement as well as a gateway for innovation. A permanent cooperation structure lies ahead, beyond the project duration.

A special Thank You! to all those who contributed so well, and one person in particular: Zale Johnson from the UK Home Office; all the best in your new job as H2020 UK representative.

Patrick Padding
Project Coordinator

Practitioners Groups Results 2019

This I-LEAD practitioner workshops bring together practitioners working within Law Enforcement Agencies across Europe. Over the duration of the project, 25 workshops will be delivered and be hosted by the project's consortium members. The workshops present a unique opportunity for experts to work as a European and consider and discuss common issues and challenges within their field. The workshops also provide a forum that facilitates open dialogue to identify 'fit for purpose' end user priorities. Furthermore, the bringing together of likeminded individuals from an international arena offers an opportunity for the real time sharing of local solutions to address national issues. The workshops also promote the development of building new working relationships and support those collaborations that already exist.

I-LEAD'S SUCCESS STORY SO FAR

In 2019, I-LEAD was successful in bringing together experts from operational law enforcement from across 17 Member States to deliver 4 subject specific practitioner workshops. These facilitated events took place in Italy, Spain, Poland and Portugal, and provided a conducive environment for participants to collaborate as a community, discuss end-user requirements, and ultimately identify an agreed set of priorities in the following topics:

- Financial Investigations - Rome
- Caine in Transit - Madrid
- Public Order - Poznan
- Digital Forensics - Lisbon

Financial Investigation – BEC Fraud

One of the financial criminal activities that falls within the realms of 'cybercrime' includes that of Business Email Compromise (BEC). Fundamentally, the criminal utilises fraudulent emails to attack organisations, by first imitating an employee within an organisation and then sending a single or a series of spoof emails to a senior colleague (CEO or similar) or a trusted customer. The email will issue instructions such as approving payments or releasing client data. The emails often use psychological manipulation to trick the victim into divulging confidential information and to make money transfers to the bank accounts of the fraudster.

For these types of crime, the cybercriminal is not focussed on attacking a mass target, as is the case with phishing. The criminal carefully selects the target using social engineering and other hacking methods to intrude a computer and deceive its victims.

For fraudulent activities such as these the cybercriminals only have to be successful a few times to generate high illegal profits. However globally, organisations are losing billions in revenue, which impacts on national and international economies. Data reveals that these amounts can be more than $2 million per fraud. According to statistics from the FBI, victims have lost $5.3 billion worldwide in the period between October 2013 and December 2016 . In 2017 alone, victims in the U.S. have lost $675 million .

Online payment frauds are complex and due to geographical diffusion of the crime, investigations are very time consuming and difficult to solve. In general, at least three countries are involved in these crimes;

• The country/countries were the IT-infrastructure (hosting servers, domain registration) is situated

• The country where 'cashing out' via money mule accounts is situated

• The country where the potential target is situated

• The country where the criminal operates from

In relation to the investigation of this type of crime, the increasing number of reports in relation to the low number of specialised cybercrime investigators within law enforcement services makes it difficult to combat. Therefore, law enforcement services across Europe need to collaborate and work closely together to find innovative solutions to inhibit and stop the cybercrime fraudster. Online payment scams are becoming more and more of a serious security and safety threat, which disrupts and undermines society. It causes huge economic losses and is diminishing trust in businesses internally and externally. Furthermore, it has the potential to endanger national and international security if criminals use the gained illegal assets to finance other criminal activities such as; terrorism, people trafficking and drug manufacture and trafficking.

Priorities of the Financial Investigation Community of Practitioners

The practitioner workshop identified a number of areas for development that would improve the approach that law enforcement has towards dealing with BEC fraud. The practitioners are from two distinct backgrounds; those that have the investigation skills to carry out enquiries related to financial irregularities; and those with technical skills in interrogating the digital aspects of the crime. The nature of this type of criminality requires investigators to become more aware of the digital world and the risks that it presents as well as the investigative opportunities it offers. As there are no geographic boundaries to online criminality, the variation in procedures, legislation and technology would benefit from harmonisation and standardisation as well as presenting a unified methodology when dealing with financial institutions and internet service providers who often hold the information that is key to successful investigations. Practitioners agreed that the current landscape for dealing with BEC crime is fragmented and would benefit from more coordination and cohesion, particularly in the following areas:

- ♦ *Better collaboration with service providers*
- ♦ *Sharing Information*
- ♦ *Multi-disciplined personnel*
- ♦ *European Working Group*
- ♦ *Stop the money capability*
- ♦ *Improved LEA collaboration*

Opportunities for Development

- Better Collaboration with service providers

Gaining information from Virtual Private Network (VPN) service providers by LEA's across Europe varies from one country to the next, with some countries having legislation in place so that obtaining information from service providers is much easier. However, even with good relationships and legislation in place the data provided is limited. Practitioners expressed a need that VPN providers should be able to provide any data that they hold including; originating IP address and machine and systems data. LEA's having access to this data would mean that they would be able to investigate a suspect/device and create improved intelligence, and also link and cross reference against other data sets. To enable this capability, it is clear that new legislation is required across Europe and an improved mutual trust between LEA's and VPN providers, additionally access to the information needs to be standardised across all Member States to ensure optimum exploitation and sharing of the data and intelligence obtained. Presently there is no technology available for overt financial investigations, and is very limited for covert around VPN's other than actual hacking tactics. Practitioners also stated that information gathering from the providers should be in real time and auditable and research and development for this discipline should concentrate on these areas.

- Sharing Information

Some of the practitioners use the European Platform for Experts however there is no consistency to this as it is deemed not user friendly. The practitioners stated that they require a future proof platform that is easy to use, secure and where they can have forum chats and exchange 'live' operational information/documentation via a desk top or remotely (mobile). It must be future proof. The ownership and management of such a platform should be by a trusted organisation that ensure security of' sensitive data' exchange including video conferencing facilities.

- Multi-Disciplined Personnel

With these types of crimes, it is important to have cybercrime expertise as well as financial expertise. It is not realistic to expect investigators to have both expertise. Therefore, it is necessary to have hybrid teams were the right expertise is brought together.

- European Working Group

In order to connect, communicate, build trust, improve knowledge and help each other on a European level, it is important to meet on a frequent basis. The practitioners looked towards ENLETS as a possible platform for a working group that would meet on a quarterly basis. The practitioners discussed a number of items in relation to this top including having a trusted group which could include the FBI to share potential threats, intelligence, trends and good practice statistics. However, it was felt that there should be a secretariat to ensure that management of such a group would have administrative support.

- Stop The Money Capability

Practitioners agreed that there should be a capability to quickly 'stop the money' of criminals which would include the closing of bank accounts, freezing accounts and seize money at home and abroad. To have this facility LEA's need to build good relationships with banks and that the UK model would be one to emulate, (this is used in Portugal and France).

- Improved LEA Collaboration

BEC is a global issue and practitioners discussed a way in which they could collaborate more and obtain information from non-EU countries. In general, it was put forward that agencies such as EUROPOL and INTERPOL could assist in this requirement, and that European LEA's should build better relationships amongst each other. This would enable a faster freezing of bank accounts abroad without the need for legal assistance, e.g. a request from a public prosecutor. Additionally, it was put forward that it would be of benefit if warrants from one country could be used in another - 'cross border warrants'.

Drug Trafficking – Cocaine in Transit

The effects of illegal drugs on individuals and society is immense and so tackling the drug problem within Europe must be a shared responsibility of all Member States. This practitioner workshop provided a forum for Law Enforcement Agencies to work as a community and work in a collaborative and cohesive way in order to contribute to the fight against the criminal activity of trafficking drugs, in particular the trafficking of cocaine.

Year upon year organised crime groups are becoming increasingly sophisticated in the way they carry out the trafficking of all types of illicit drugs. This is demonstrated by the exploitation of legal technologies such as prepaid phones and the internet, which they use to maintain control and keep track of these illegal and valuable consignments. This adds to the complexity of the crime as remote drug trafficking means that the trafficker can maintain anonymity at all times. This is challenging law enforcement in ways never seen before, alongside a number of other factors and considerations which must be taken into account during an investigation. For example; border controls, money laundering, covert surveillance, intelligence (of routes and organisations), exchange of information among LEAs, communications used by criminals (encrypted and open ones) and sensors and scanners to detect drugs in transports, etc.

Priorities of the Drug Trafficking Workshop Community of Practitioners

Despite the use of technology by the traffickers, the drugs themselves remain in the physical world and have a physical entity that require successful transportation from country A to country B in order for the criminal to reap the monetary benefits. Vulnerability for Organised Crime Groups (OCG's) exists along the whole chain of cocaine transportation. From the loading onto bulk vessels to when it is decanted from the shipping containers, which often entails the concealment of smaller consignments within specially designed hides in smaller boats and/or vehicles. These vehicles are then used to convey the cocaine to safe-houses or across land and coastal borders. It is this area that the practitioner workshop focused on; the detection of cocaine within shipping containers and within vehicles. Some of the areas discussed and considered are shown below;

- ♦ *Exchange of information between countries*
- ♦ *Intelligence systems - to better detect organised crime groups and their trafficking routes*
- ♦ *Communication interception technologies for open and closed sources, including email telegram, Instagram and Facebook*
- ♦ *Cross border surveillance and tracking*
- ♦ *Detection of drugs in containers*

Opportunities for Development

- Exchange of information between countries

Practitioners expressed the desire to have the ability to share information with colleagues from other agencies, countries and across borders in real time using a dedicated sharing platform. It was emphasised by the LEA practitioners that theirs is a common fight against drug trafficking across the EU and that the sharing of open source information (not intelligence or evidential) would be beneficial to all and sharing good practices would save money and time. Furthermore, sharing information with regards prior knowledge of logistic organisations and shipping companies would also be of use to identify deviations of transportation trends that may indicate potential criminal activity.

- Intelligence Systems

The drug trafficking investigator would like to have better links into OSINT and improved tooling including that of being able to decrypt mobile devices and apps, better search the internet and patrol the dark web, be able to interrogate blockchain and crypto currencies and use SIGINT to process signals of interest and extract relevant data.

- Communication interception technologies

Practitioners discussed the challenges faced when criminals used encryption as a means of ensuring that their communications were secure from any intrusive investigation. It is common to see encrypted Apps such as Signal and Telegram being used which current law enforcement methods find difficult to access effectively. Also, the use of encryption within devices can prevent the interception of mobile telephony. Criminals routinely have access to high end communications technology that they frequently update or change more rapidly than law enforcement can respond to therefore tools are required that enables advanced communication interceptions to be available. During the workshop discussions practitioners agreed that an International Mobile Subscriber Identity Catcher (IMSI- Catcher) would reap great benefits in the surveillance of drug trafficking criminals. Having this capability would mean that once the targets phone was in range and connected to the IMSI the police officer could better locate and track the person of interest using Radio Frequency (RF) Mapping. Moreover, LEA's would like to work more closely with mobile phone companies so that they can assist with drug trafficking investigations. Additionally, practitioners would like the capability to exploit and hack into a vehicle's computer.

- Cross border surveillance and tracking

The highest demands for increased capability were in the surveillance and tracking areas with a number of key issues identified including:

Real time monitoring of vessels at sea - At present there is no 'real-time' monitoring of sea vessels, as any satellite imageries obtained are delayed post detection of a suspect vessel. Drug trafficking investigators would like to have a global maritime system with vessel positioning that they could access less than 1-hour post detection. This end-user priority should also be extended so that maritime data in relation to the vessel under investigation should be available, such as crew details, intended routes and schedules.

Drones - Practitioners stated the need for improved mobile surveillance technique in particular, the use of drones for information capture could have a significant positive impact in the fight against drug trafficking. The end-user future requirement for drone technology should have improved capabilities that is non-detectable and include enhanced imaging technologies such as a Remote Video System (RVS). Additionally, practitioners require sensor capability (electrical and physical) so that persons of interest could be detected, monitored and tracked in real time and at a distance whatever the environmental conditions and situations. Other additional capabilities that could be mounted on drones were put forward by the practitioners were those of Artificial Intelligence and Facial Recognition, however it was recognised that additional drone capabilities would require a greater power and a longer battery life; e.g. months; to maintain continuous surveillance over a longer period of time and over a greater distance. This would avoid sending officers into the field and putting them at risk of detection by the criminals. The practitioners also stated that the cost of these capabilities should be kept to a minimum so that it was available to all LEA's whatever their budgetary means.

Audio - During the workshop discussions, practitioners put forward that they would like to be able to capture clear audio evidence covertly, at distance (500mtrs) and through walls, to avoid having to go into a building to set up listening devices. Improved efficiency of micro array recording would also be of benefit to obtain surround sound recording throughout a room and better know the positioning of those talking, be more accurate of who is talking and to omit background noise. Practitioners put forward that they would also like to utilise automated lip-reading technology and sound vibrations, during investigations and that they would welcome development in both these areas in order to assist in a surveillance situation and be used as evidence in a court of law.

Disposable Trackers - Practitioners expressed that they would like to have a long life, low cost single use GPS tracker that can be fixed to all types of vehicles. This would be of great value to the investigator as there would be no need to retrieve the device once it has been used, which would reduce the chance of being detected by the criminal.

- Detection of drugs in containers

Detection is a high priority for LEA's and encompasses several different areas including the detection of concealed drugs within; containers, vehicles, buildings and people, for example an 'electronic sniffer', a device that could identify a substance using a rapid chemical process such as chromatography. Once detected the practitioners would welcome the ability to have real-time in the field analysis, and rapid automated screening of suspicious substances.

Public Order

It is recognised that across Europe and elsewhere the scrutiny placed upon law enforcement when policing public events and dealing with disorder has never been greater. This is particularly true for large gatherings that are held under the gaze of the media, whether that is via traditional means such as television or via the internet and social media sites.

Traditional "public order" styles of policing are ostensibly reliant on control of an event or a crowd and are increasingly being seen as inappropriate, unaffordable or not in accordance with an evolving ethical approach to policing that seeks to put consent and facilitation to the fore. In some countries, this has coincided with significant reductions in funding to policing that has in turn reduced the capacity of the police to undertake significant and prolonged public order deployments.

Consequently, policing and other law enforcement agencies need to consider how they might better use science and technology to assist them to provide public safety. A number of key areas for consideration are:

- *Development of information on the event*
- *Development of information on the intelligence of those attending*
- *Resultant crowd size and dynamics*
- *Numbers, training and equipment of police resources*
- *Briefing and deployment of police resources*
- *Information channels to / from individuals, groups and the crowd in general*
- *Dynamic direction and control of police resources*
- *Dynamic monitoring of the event for operational purposes*
- *Enabling dynamic public scrutiny of the event and the police response to it*

Given these factors, what can current and future developments in science and technology bring to enhance the police's understanding of the crowd, its intent, capacity and capability and how can this understanding then be better used? The workshop considered this across a number of different scenarios and through the timeline of each: a major sporting event; a major festival or concert and a significant protest or demonstration, all involving at least tens of thousands of people. In particular:

- *What technical assistance would better inform the police's intelligence on and perception of the crowd and inform the graded use of available tactical options with a view to maximising engagement and mutual understanding and minimising the use of force?*
- *How could social science or technology and training, alongside evolving work on the psychology of crowds, better empower policing to promote the self-regulation of crowds and / or bring about early de-confliction of tension or "flashpoint" issues?*
- *How could technology assist with the tracking and understanding of the actual / current capacity and capability of policing assets at such an event?*
- *How could technology assist in building legitimacy for policing actions?*

Establishing potential benefits and how these might be realised is a major part of any such forward thinking strategy, although in parallel it is equally important to identify potential risks and how these might be mitigated. It is also important to recognise that there needs to be a will to work toward a greater level of integration and interoperability between agencies to maximise efficiency and reduce costs. This may for example take the form of systems and processes that are shared between agencies or that have wider uses than simply in public order or protest situations.

Priorities of the Public Order Community of Practitioners

The practitioner group identified a number of areas for development and it was clear that the opportunities for standardisation were probably greater in this PG than most of the others. The commonality between the roles carried out in each police force was evident which led to a general consensus in that the focus was public safety. There was a general move away from direct confrontation with those committing public disorder towards a less provocative approach seeking to minimise the impact through social means and exploiting technology. In addition, the lack of standards for equipment particularly that used for the personal protection of officers was raised as a priority. Other areas for development included:

- *Tracking and monitoring of known offenders*
- *Drones*
- *Decision making*
- *Communications*
- *Police and public partnership*
- *Equipment*

Opportunities for Development

- Tracking and Monitoring

During the workshop practitioners stated that facial recognition was not being utilised to its fullest potential and that there was a great opportunity to capitalise on this type of technology within public order operations. The practitioners put forward that one way in which facial recognition could be used, was to identify person or persons who had previously been identified as an offender, and one who had the potential to cause disorder and incite others to do the same. However, practitioners were aware of the potential risks of using this technology, and that is the possibility to alienate those law-abiding citizens who had no inclination or desire to cause disorder. Therefore, it was stated by the community that any business case or research put forward to facial recognition systems with a public order arena should take into account the social and ethical implications prior to its use.

- Drones

Although a number of the Law Enforcement Agencies across Europe presently use drones within a public order scenario the practitioners agreed that there was one major pitfall around their use. This being; not having the ability to integrate all the information collated from the drones (and other sources) into one system, which impacted on strategic and operational decision makers. Practitioners also expressed a desire for drones to have an 'artificial intelligence' capability that could provide a prediction or indication of an outbreak of public disorder during large scale events. For example; with the use of algorithms it could be possible to determine if a crowd or an individual person was acting in an irregular manner or using language, movements or voices that was a precursor to violence.

- Decision making

The use of Artificial Intelligences within decision making is being used more and more across many business sectors especially in areas where large amounts of data needs to be gathered and analysed. AI can process more data than any person and can make better and faster predictions without the bias and emotions of a human being. Furthermore, via the collected data, AI can identify patterns in a way that humans cannot, and this can be done faster and more accurately. Therefore, it was put forward that the use of Artificial Intelligence in a public order scenario to analyse the large amounts of data sets in real time would be of great benefit. This capability would allow the public order police officer to deploy personnel and equipment to the right place and at the right time and have the potential to diffuse a hostile situation before it occurred. This would require existing systems to be more integrated and feed into one repository rather than buying a new system that forces could not afford.

- Communications

Practitioners agreed that following a large scale public order operation there is often too much information to consider, assess and analyse. Having the ability to filter out the most important information would be of great benefit and less time consuming for Law Enforcement Agencies. Presently the radio technology and cellular networks provide a suitable means of communication however police officers need to have more control over what information is important and what is inconsequential. Having an automated system that distinguishes between the two would be of great value and would also mitigate an overloading of systems. Furthermore, the group added that communication systems are set up to deal with 'normality' and not for major public order incidents and therefore to have a system that could 'identify' when large amounts of transmissions occurred and then alter its status to deal with this, would be of great benefit. Practitioners agreed that following a large scale public order operation there is often too much information to consider, assess and analyse. Having the ability to filter out the most important information would be of great benefit and less time consuming for Law Enforcement Agencies. Presently the radio technology and cellular networks provide a suitable means of communication however police officers need to have more control over what information is important and what is inconsequential. Having an automated system that distinguishes between the two would be of great value and would also mitigate an overloading of systems. Furthermore, the group added that communication systems are set up to deal with 'normality' and not for major public order incidents and therefore to have a system that could 'identify' when large amounts of transmissions occurred and then alter its status to deal with this, would be of great benefit. It was recognised by the group that some of the issues experienced are not all technology related and could be reduced by adopting an improved and more efficient communications strategy, having better defined requirements and thinking differently how communications are managed. Although there concerns amongst the group in relation to the introduction of 5G and the impact this will have on policing. The next generation of mobile internet connectivity will bring new challenges, especially as it will provide a means of faster sharing of information, thus bringing new and interesting challenges to Law Enforcement Agencies. Additionally, the group agreed that 'lessons learnt' post public order events in relation to communications should be shared with colleagues across Europe in order that improvements are made easier and faster.

- Training

The practitioners attending the Public Order workshop put forward that there needs to be more exchange of information on working practices and to work alongside each other to gain an understanding of the challenges faced in different countries during operations. They stated that more novel ways of delivering training in the future should be investigated e.g. YouTube, e-learning and translation of training programmes into different languages, and perhaps that the CEPOL's on-line training courses good be a good starting point. The group stated that they would like to build the network and share ideas and lessons learnt more efficiently using an on-line platform. Practitioners pointed out research shows that more focus on low level tactics would reduce high level public order activity, and that more training in this area would be of great benefit. However, there remains a need for high level training in preparedness for these types of operations and that although these didn't happen very often training should be continuous and regular to maintain the appropriate skill, knowledge and ability.

- Equipment

All participating forces are responsible for the selection and purchase of equipment utilised by police officers involved in public order duties. Equipment falls into several categories; personal protective for individual officers; front line equipment; vehicles; and information gathering. All are utilising similar type equipment but there is no European standard in place for protective equipment. There is a reliance upon local standards in some cases and most were not subject to a robust testing procedure against those standards that exist. There is significant scope for the development of a European standard for public order equipment that would ensure that all police officers are being protected to a common minimum standard, but also opens the door for interoperability between countries and the potential for common procurement across multiple countries.

Digital Forensics

Digital Forensics (DF) is a relatively new science but is evolving rapidly in order to keep up with exponential technological developments. It supports other related areas of judicial investigation, such as, e.g., cybercrime, which often build upon the base layers of investigation as offered by digital forensics. From either the purely technical approach of looking at the field of digital forensics, as well as from the more theoretical point of view, it is clear that the DF field still finds itself confronted with various issues such as:

- *a continuing expansion, in terms of both the type and the number of different (mobile) devices submitted as evidence*
- *a seemingly ever-increasing amount of raw data being stored on these devices and media*
- *an abundance of file and data formats*
- *various tools, protocols, standards, and implementations thereof that may also deviate from their originally intended specifications or requirements*

This area of work is rapidly and continuously evolving, this alone makes it difficult for practitioners to work within the discipline of DF. Moreover, maintaining momentum of handling real casework and implementing the required training and educational aspects, whilst upholding and updating quality assurance methods and procedures are a challenge.

Another issue for the DF investigators is the handling and management of large amounts of data, which instigates the utilisation of somewhat ad hoc triage and data elimination strategies. This in turn has the potential to limit the technical depth of an investigation and increase the risk of misinterpretation and incomplete or incorrect processing of forensic evidence.

Additionally, as consumers are requiring more data security and privacy, their concerns are pushing forward the use of encryption and other protection measures which makes it more difficult for LEA's and other investigators to obtain basic access to the required stored data. Furthermore, data storage is no longer solely “device oriented”; evidence may be stored “in the cloud”, i.e., on remote servers in other jurisdictions for which both technical and legal measures and procedures need to be made available.

Due to the sheer volume of data that needs to be processed, DF practitioners are also increasingly becoming dependent on their automated lower-level tool sets for which the performance and general reliability has often not been fully or independently evaluated and publicly reported on. Hence, many practitioners often apply, e.g., in-house testing procedures, or resort to the use of two or more tools to “cross-validate” them or (compare and) merge the obtained sets of results.

At the other end of the DF tool spectrum similar issues may need to be considered for recent developments in “big data” and “machine learning/artificial intelligence” tools; how could or should such state-of-the art tools be tested and evaluated, in order to properly support the judicial process at large?

Increasingly, these questions seem to be inspired by the DF fields' desire and need to implement quality assurance considerations and standards (e.g. ISO17025). Some government owned LEA and forensic institutes are struggling to both recruit and retain staff members which are both able and willing to sustain the case work stress levels and back logs, whilst the field continues to evolve as already indicated above.

Priorities of the Digital Forensics Community of Practitioners

The workshop covered a broad range of issues including the balance between the front line initial responses by investigators, the highly specialized in-house LEA or forensic institutes' case work, and possibly outsourced or subcontracted handling of investigative tasks by external companies or academia. International collaboration across EU MS may offer an alternative or supplemental solution for some of these issues, but further standardisation of forensic and judicial standards and procedures, as well as fluent administrative and low overhead administrative procedures may then need to be explored further. Participants considered real-life problems experienced by LEAs in EU MS, including both technical, quality assurance, workflow and DF laboratory management responsibilities as well as developing or anticipated new technologies, methods, strategies, or standardisation and other efforts that may help to further advance the field of DF. The priorities can be categorised as:

- Password cracking and encryption
- Artificial Intelligence and machine learning
- Training and expertise
- Sharing of data and information

Opportunities for Development

- Password cracking and encryption

The practitioners agreed that a common problem within digital forensics are the challenges with regards encryption of devices and password cracking. Decryption is a time-consuming process and so to be able to do this task quicker and more efficiently would be of great value. It is foreseen by the digital forensic practitioners that there will be more and more different types of encrypted devices in the future especially with the introduction of 5G. Additionally, the storage size within devices is becoming larger and therefore able to hold more data; that is to say more potential evidence that can be used within criminal proceedings. Additionally, the ‘cracking’ of passwords is equally as crucial to investigate the data within a device. Presently the dictionary of words used as passwords is not adequate and this needs to be built upon and shared amongst practitioners. It was put forward that the construction of ‘smart dictionary’ algorithms that could create glossaries of terms and words from the details of a case would be an advantage for the investigator. It is both these areas of work that the practitioners believe would benefit from funded research and development, and “futures” analysis, as most crime has a digital element, and keeping ahead or at the very least, up to date with the technology in this field will be vital to ensuring successful prosecutions.

- Artificial Intelligence and encryption

As the workload, time constraints and challenges of the Digital Forensic Practitioner increases to attain a successful conviction, more and more police forces are looking towards the exploitation of Artificial Intelligence and/or Machine Learning to better fight criminal activity. The tools used by the Digital Forensic Investigator are very often, not fit for purpose, with no present solutions for big data and triage of big data which is getting increasingly complex. The ‘splitting’ of tasks between several tools; commercial and open source, causes major problems and therefore a multi-functional and integrated tool would improve all areas of the work. One practitioner stated that, “Even with good computing power, commercial forensics tools fail when they have to deal with a large amount of data. The solution to this is the integrated use of several tools, commercial and open-source, splitting, if possible, the data to be analysed in smaller blocks and correlating the results, under the penalty of losing some relevant information and spending more time in case analysis”. Therefore, one of the solutions to this, would be for the Digital Forensic Officer to employ Artificial Intelligence. The use of a ‘less manual’ technology with a more smarter thinking capability would enhance the way large amounts of data is dealt with and provide the Officer with an optimised evidence extraction tool. The areas in which Artificial Intelligence could be used for example is for the: speeding up the reviewing of data and potential evidence from multiple devices, including images/videos; to differentiation between relevant and non-relevant data sets and to identify key evidence at the earliest opportunity.

Other areas in which Artificial Intelligence could be utilised is: the mapping of connections between people of interest; building timelines of the activities of potential criminals; analyse context from conversations and integrate data from multiple sources. It may be even possible to apply Artificial Intelligence to identify and transplant a component part of a device that has been maliciously or accidentally destroyed, and that has the potential to assist in the investigation of a crime.

- Training and expertise

The Digital Forensic Practitioners attending the workshop were all keen to express the need for a more formal approach to the discipline and in the words of one of the practitioners, 'to provide a more professional service to the Criminal Justice System and have less ad-hoc processes and procedures'. Furthermore, it was seen that the key to this requirement was to have a structured education programme, and during the discussions it was put forward that the discipline would greatly benefit from having a dedicated centre of training for the Digital Forensic Technician for which education grants would be available. The practitioners stated that at present it is difficult to take on and keep good staff and it was believed that this was partly due to the discipline not having a framework of learning and ongoing standards of competency. Additionally, highly knowledgeable staff were leaving digital forensics as their expertise could earn them more money in other business sectors. With regards the type and mode of training tools the practitioners put forward a number of solutions, these being; e-learning and classroom based training and practical exercises. However, as there are thousands of Digital Forensic Officers around Europe who require training it was proposed that the use of Virtual Reality technologies could provide an on-line dedicated training capability for the masses in a simulated environment. Additionally, this training could be easily standardised and thus formalising processes and improving the integrity and quality of digital evidence using 'good practice' throughout Europe. It was also deemed that there should be different levels of digital forensic responsibilities and abilities, for example: expert/specialized and general/non-specialised each having specific role requirements and ensuring that the recruitment process was clear and unambiguous, and the developmental progression of the digital forensic examiner was that which allowed employment progression.

- Sharing of data and information

During the discussions amongst the practitioners it was found that there were two aspects to the sharing of data/information; the first being the sharing of information amongst the community of practitioners in relation to the promotion of good practices and procedures and problem solving etc. The second being that of sharing evidential data including that in relation to criminal investigations.

Sharing Data

With regards the sharing of data, is was believed that due to the lack of efficient data sharing, opportunities for the sharing of evidence and intelligence nationally and internationally, were being missed and therefore the opportunities for the successful convictions of perpetrators of crime. To have a networked intelligence and evidence sharing capability for Law Enforcement Agencies would be of substantial benefit to the investigative process and should include the technology to share reports, images and intelligence for review and evaluation.

Sharing Information

The community would require that registered forensic experts could have a facility that gave them the opportunity to chat in real time and to share experience with each other. They required the functionality to be able to discuss and assess the 'tools' used by the Digital Forensics Officer and to make more informed decisions when considering using or buying such tools. Being able to discuss the pro's and con's of different commercially available and open-source tools would be a great asset and save time and effort.

Both of the issues highlighted above, could be improved via an on-line platform (community information sharing) and a centralised server for collection, analysis, dissemination and management of data, (evidential and intelligence sharing). Both of these, it was suggested should have remote accessibility for officers and have an easy to use interface.

In 2019 the practitioner workshops have proven to be extremely successful, and has been evidenced by the identification of a list of key priorities. These priorities were attained through careful and methodical discussions amongst the practitioners and moreover have been found to be new and unique requirements that have not previously emerged from the policing community. The impact of these findings will contribute to the formation of a set of 'grand challenges' for those who seek to find or undertake research to address the issues. Thus, directing those to produce 'fit for purpose' solutions and to improve the way LEA's fight crime and keep citizens safe and secure. We now look forward to the 2020 workshops and are confident these will be as successful as those previous.

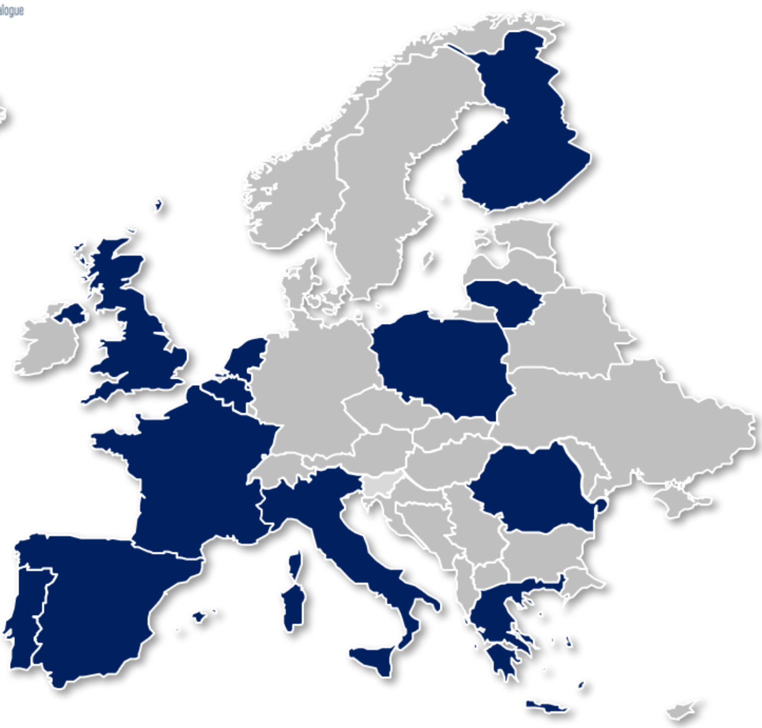
Read the PG Report 2019 in our website:

www.i-lead.eu

www.i-lead.eu

i-LEAD Partners

innovation - law enforcement agency's dialogue



Visit our website: **www.i-lead.eu**

YEAR	PRACTITIONER GROUPS and TOPICS				
	Front Line Policing PG 1 - UK	Cross Border PG 2 - Spain	Cybercrime PG 3 - Netherlands	Crime PG 4 - Romania	Forensics PG 5 - Belgium
2018	Mobility for officers 20th – 21st February	People trafficking 14th – 15th March	OSINT 17th – 18th January	Intelligence analysis 14th – 15th June	Emerging DNA technologies 20th – 21st September
2019	Public order 28th - 30th May	Drugs Trafficking 8th - 9th May	Financial Inv & Virtual currencies 23rd - 24th January	Digital Investigations 10th - 11th September	Digital forensics 26th - 27th June
2020	Vehicle Mitigation 18th - 19th November	Firearms crime 17th - 18th June	Cyber extortion 23rd - 24th September	Inf. Management Machine Learning & Principles 22nd - 23rd April	Crime Scene Recording & Documentation 11th - 12th March
2021	Technology in vehicles (TBC)	Child sexual exploitation (TBC)	Biometric verification (TBC)	Surveillance (TBC)	Future Individualisation techniques (TBC)
2022	Police use of firearms (TBC)	Counterfeit goods (TBC)	Credit card fraud (TBC)	Crime prevention (TBC)	Drug analysis NPS (TBC)

Industry Days 2019 in Helsinki

Partners of i-LEAD, members of Industry and interested LEAs from around Europe came together on the 5th November for the first edition of i-LEAD Industry Days in Helsinki, Finland.

The concept of Industry Days is to connect practitioners with the providers of technology software and systems recognised by the project as key focus areas in individual streams of law enforcement. Bringing these stakeholders together creates an atmosphere for constructive dialogue aimed at addressing innovation gaps faced by experts.

The i-LEAD Methodology

A series of workshops ran during the project helped the Work Package 2 team elicit the gaps and challenges encountered by LEAs. Cooperation between the work packages responsible for the workshops, and those managing the analysis of technologies allowed the event team to target specific companies to apply for attendance.

Once each of the applications was reviewed and evaluated by experts from each domain, fifteen companies covering seven different technology areas were invited.

At the event, each company provided overviews of their technology and solutions to interested audience members. The attendees were mainly from a selection of Law Enforcement Agencies and research institutions.

The technology companies each had two, one-hour slots, to present their products and detail their key features and benefits. Besides, the time provided an opportunity to dive into more specific details about architecture and security and other related content. Each presentation was concluded with a question and answer session.

Interact with the technology links below to find out more about the 15 companies who delivered presentations and interactive sessions at Industry Days.

As this was the first edition of Industry Days, the event was not perfect. It was a proof of concept that can be altered and improved before the next iteration. That said, the event was generally received well, and attendees and technology presenters were satisfied with the interactions.

Event Rationale

The overarching goal of i-LEAD is to build connections between industry, technology experts and LEAs. This will help to develop strong communicative networks that encourage acontinued dialogue for innovation, procurement and improvement initiatives.

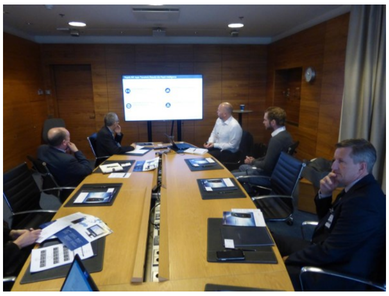
Industry Days was designed to support this approach.

The event was created to support the output of the Practitioner Workshop Report (PWR) from 2018. The PWR identified numerous gaps and opportunities for improvements in the technology used by Law Enforcement.

Workpackage 3 (WP3) of the i- LEAD project, is dedicated to monitoring research and innovation related to security technology solutions. This group was responsible for the work involved in organizing and preparing Industry Days.

Each of the technologies monitored by WP3 relates to specific streams of Law Enforcement, and were categorized as:

- **Open Source Intelligence (OSINT) Tools**
- **Police Vehicles**
- **Drones**
- **Facial Recognition Systems**
- **Online Speech Translation Tool for Different Languages**
- **Rapid DNA - Faster Results**
- **Body Fluids -Automating the Stain Search**



Event Methodology

The origin of the event came from internal discussions between workpackage leaders and the coordinator within the i-LEAD project.

Together, the decision was made that ‘Industry Days’ would take place in 2019 and organized to coincide with the Security Research Event in Helsinki. Combining these two events increased the value for the attendees.

A formal concept for the event was designed and published to the public in July 2019. The document aimed to outline the purpose of the event and to motivate interested Technology Partners to apply for a presentation slot at the meeting.

Numerous applications were received from technology companies throughout Europe and one in the United Stated.

The technologies represented most of the target areas but some of the desired topics were not adequately covered.

The categories included:

- **OSINT**
- **Intelligence Analysis**
- **Facial Recognition**
- **Drones**
- **Rapid DNA Testing**
- **Police Vehicles**
- **Video Management**

i-LEAD Industry Days strived to be different from other events. Providing a smaller number of technology providers extended, dedicated opportunities to explain their product's unique value points in depth. Deeper engagement allowed for more useful discussion. Meaning the presenters got to the core of the technology. This approach also provided ample opportunity to ask questions during each session.

Read the full report in our website:

www.i-lead.eu

i-LEAD Events Participation

i-LEAD at Polish LEAs meeting – Warsaw, Poland

On 24-25 April Polish Platform for Homeland Security organized a two-day meeting with Polish LEA to present Horizon 2020 in practice.

The i-LEAD Project is one of the good examples of projects carried out by LEA, including Polish Police, which was extensively presented and discussed during the meeting.

i-LEAD at International Defense Fair (FEINDEF) – Madrid, Spain

i-LEAD successfully participated in International Defense Fair (FEINDEF), hosted at the booth of Spanish National Police and Guardia Civil which was held between 29th-31st of May in Madrid, Spain.

i-LEAD showcased its results and activities, attracting the interest of the attendees of the fair.

The booth where i-LEAD was presented was visited by the Spanish Minister of Science, Innovation and Universities, Mr Pedro Duque and the Spanish National Police General Director who encouraged the partners of the project to continue working in this successful way.

i-LEAD Workshop "Procurement for Innovations in the Area of Security" - Delft, Netherlands

i-LEAD project successfully organized the workshop titled: Procurement of Innovations in the Area of Security. The workshop took place on the 23rd of May 2019 at The Netherlands Standardisation Institute (NEN), in Delft, Netherlands.

The main idea of the workshop was to discuss about current experiences and challenges in procuring innovative solutions, dedicated especially for Law Enforcement Agencies and other institutions responsible for security.

The following topics were raised during the workshop: Pre-Commercial Procurement (PCP), Public Procurement of Innovative Solutions (PPI), Innovation Partnerships.

i-LEAD Co-organized Mediterranean Security Event MSE2019 – Fodele, Greece

i-LEAD project successfully participated as a Co-organizer at the Mediterranean Security Event MSE2019, which took place between 29th – 31st October 2019 at Fodele, Greece.

I-LEAD Project Coordinator Mr. Patrick Padding presented the vision of the project along with its results and achievements within the first two years to an audience of approximately 250 people. Mr. Patrick Padding also presented the “Law Enforcement Priorities in the era of new digital tools” through i-LEAD participation under the thematic section “European Initiatives on Security and Networks of Practitioners”. Right after the presentation a Q&As section followed attracting the interest of the project stakeholders and EU officials that attended this panel.

i-LEAD in collaboration with MEDEA project co-organized the “Workshop on fighting crime with focus to drugs and people trafficking” in which the end user and stakeholders actively participated interacted while interacting with actual scenario-driven situations with respect to the workshop topic.

i-LEAD Events Participation

i-LEAD General Assembly (GA) Meeting - Helsinki, Finland

i-LEAD project held its General Assembly (GA) Meeting on the 6th of November 2019 in Helsinki, Finland. The meeting was attended from the project partners and were extensively discussed the achievements the project so far.

The project coordinator Mr. Patrick Padding of the Netherlands Police evaluated the project's outcomes during the 2nd year of its operation and pointed out the adjusted guidelines which will further sustain the successful course of the project.

Furthermore, planning for future activities of the Consortium partners has been set and discussed among the various WP tasks.
The i-LEAD WP Leaders delivered presentations in detail regarding the conclusions derived from i-LEAD 2nd year and discussed with the Consortium assembly the planning of the forthcoming period.

i-LEAD in "Boosting Innovation through Standards" – Brussels, Belgium

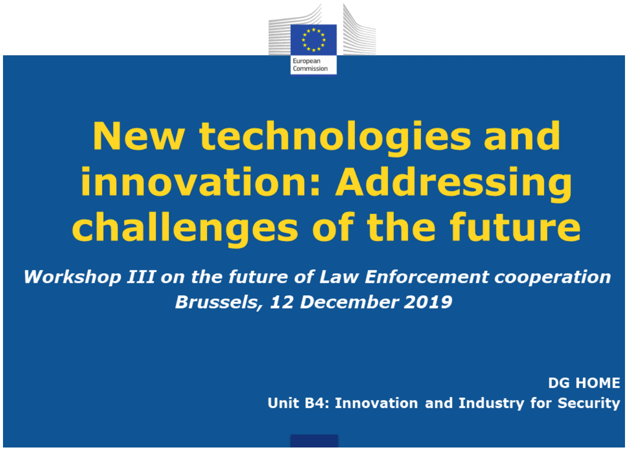
i-LEAD successfully participated at "Boosting Innovation through Standards" which took place in Brussels on the 13th of November. This high-level event main objective is to boost the market uptake of innovation and research outcomes by using standardization as an enabler.

i-LEAD was hosted at NEN (www.nen.nl) exhibition booth and attracted the interest of the event participants. Leading experts in innovation and standardization presented had contacted our Project partners at NEN, Ms. Leanne Valom and Ms. Merel Haverahls and have been informed relevantly to our i-LEAD project achievements.

Workshop III on the Future of Law Enforcement Cooperation, Brussels - Belgium

i-LEAD successfully participated represented by the Project Coordinator & Core Group Leader of ENLETS Mr. Patrick Padding at the “Workshop III on the Future of Law Enforcement Cooperation.” The workshop was organized by European Commission DG MIGRATION and HOME AFFAIRS and took place on the 12th of December 2019 in Brussels, Belgium.
The most important topics regarding the future of Law Enforcement were extensively discussed giving emphasis to the:
- Empowerment of SPOC as "one-stop shop" in accessing and exchanging international law enforcement information
- Analysis of information for strategic, tactical and operational purposes
- Addressing challenges of the future in terms of New Technologies and Innovation

The workshop was chaired by Mr. Rob Rozenburg, Head of Unit Police Cooperation & Information Exchange

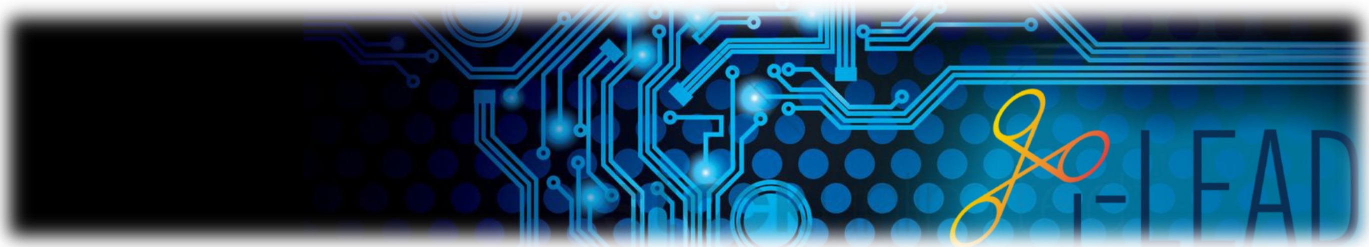


European Commission

New technologies and innovation: Addressing challenges of the future

Workshop III on the future of Law Enforcement cooperation
Brussels, 12 December 2019

DG HOME
Unit B4: Innovation and Industry for Security



Upcoming Events

11th - 12th March 2020 **Crime Scene Recording & Documentation Practitioners Workshop** , Belgium

22nd - 23rd April 2020 **Digital Investigations Practitioners Workshop**, Lithuania

17th - 18th June 2020 **Firearms Crime Practitioners Workshop**, Czech Republic

23rd - 24th September 2020 **Cyber Extortion Practitioners Workshop**, Greece

18th - 19th November 2020 **Vehicle Mitigation Practitioners Workshop**, Finland

http://www.i-lead.eu

i-LEAD

innovation - law enforcement agency's dialogue

i-LEAD is funded by the European Union's Horizon 2020 - Research and Innovation Framework Programme, under grant agreement no 740685