i-LEAD

innovation - law enforcement agency's dialogue

innovation

Practitioner Workshops Report 2019

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

INTRODUCTION TO THE I-LEAD PROJECT

The I-LEAD project is funded by the EU Commission Horizon 2020 (H2020), 2016-2017 Work Programme under the heading of, "Secure Societies – Protecting the Freedom and Security of Europe and its Citizens". The I-LEAD project commenced in September 2017 with a duration of 5 years, coordinated by the Dutch National Police (NPN). Consortium members include 12 Law Enforcement Agencies (LEA's) and 7 research institutions who represent 13 Member states.

I-LEAD builds upon the work of the European Network of Law Enforcement Technology Services (ENLETS) that brings EU law enforcement together to share best practices, activate co-creation and stimulate research for operational purposes.

I-LEAD's key focus is to contribute to the development of new and existing crime fighting capabilities of LEA's across Europe. I-LEAD will achieve this objective by firstly, engaging and consulting with operational police officers and supporting staff from all Member States. This will be undertaken via a series of bespoke practitioner workshops, that have been exclusively designed to identify and define end-user priorities in 25 subject specific areas of law enforcement. The findings from the workshops will be used to identify 'fit for purpose' solutions within the market place, and/or direct research and innovation within academia, with Small and Medium-sized Enterprises (SME's), and/or those organisations within the security industry environment. The overall results of this work will effectively contribute to the development and enhancement, where relevant and required, of the existing policing 'crime fighting tool kit'.

I-LEAD will also examine and recommend opportunities for standardisation and joint procurement, concentrating on the technical, human, organisational and regulatory elements. This work aims to produce a positive impact that will improve connectivity and enhance interoperability between European LEA' s.

I-LEAD recognises that science and innovation have a leading role to play in the future of policing. However, history has taught us that it is the policing community that should be giving direction to this work. It is this very principle that lies at the heart of the I-LEAD project, and embraces the 'triple-helix' concept, that being; promoting a pro-active collaboration between law enforcement, the scientific community and industry. Having this conviction will ensure that maintaining public safety and security for all citizens across Europe is optimised.

The need to identify, develop and implement technologies and methodologies within the security arena to support policing across Europe has never been as vital to society as it is at this present time. Therefore, I-LEAD will be committed to undertake an active role in the future of policing by contributing to the momentum of partnerships between policing and research and innovation.

WELCOME FROM OUR PROJECT COORDINATOR

Patrick Padding

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.

OUR VISION

I-LEAD's primary vision is to support European policing and contribute to the safety and security of all citizens of Member States, through its building of enduring, collaborative partnerships between European Law Enforcement Agencies, SME's, industry and academia.

OUR MISSION

I-LEAD's mission is to not only meet, but exceed the objectives laid down in their programme of work and act as the fundamental component to ensuring that the security priorities of LEA's across Europe are realised.

SAFER COMMUNITIES FOR ALL EUROPEAN CITIZENS

The key driver for the I-LEAD project is the safety and security of all European citizens including those visiting from around the globe. It is vital that the highest possible standards are achieved, and this can only be done by ensuring that police services, academia and industry pool all available and significant resources, and work in close partnership. This will ensure that initial innovative solutions and the emerging technologies and methodologies to address the public safety issue are unrivalled, second to none and remains relevant. Furthermore, I-LEAD's work demands that there is a continuum of research and development to guarantee that all criminal activity is not only adequately and speedily dealt with, but that law enforcement agencies are one step ahead of the law breakers.

THE WORK OF I-LEAD

There are a number of major strands of work being undertaken within the project and these are as follows:

European Law Enforcement Networks

I-LEAD will establish a sustainable and permanent cooperation framework; (preferably with a legal entity endorsement), that will represent European LEA's. This will be based on the insights and mechanisms developed within the I-LEAD project. Its programme of work includes the following:

- Monitor research and innovation
- Standardisation and procurement recommendations
- Improved collaboration with industry and research
- Capacity building and knowledge exchange

Dissemination and interaction with other networks

Common End-User Priorities

I-LEAD will investigate end-user; capability gaps, baseline capabilities and the current use of technology in the respective law enforcement practitioner groups and identify policing priorities.

Monitor Research and Innovation

I-LEAD will conduct smart monitoring of relevant research and innovation projects, undertake technology watch activities and scan pipe-line technology including those in other security domains and sectors (e.g. defence and intelligence and health). Additionally, an assessment of promising technological solutions will be provided to LEA's in the Member States.

Standardisation and Procurement Recommendations

I-LEAD will investigate appropriate ways in which standardisation in Law Enforcement domains can be achieved, and where required 'make it happen'. Additionally, I-LEAD will make recommendations for LEA's in relation to collaborative procurement, based on the scanned technology and PCP and PPI.

Improved Collaboration with Industry and Research

I-LEAD will set up community forums for enhanced knowledge exchange between the project and EU LEAs, research organisations, SME's, industry and academia.

Capacity Building and Knowledge Exchange

I-LEAD will build and maintain project repositories for knowledge exchange and

provide a pool of resources to support relevant activities. I-LEAD will act as the gateway for interaction with external partners in Europe by enabling peer to peer exchanges, answering questions on LEA innovation needs and providing expert advice.

Dissemination and Interaction with other Networks

I-LEAD will establish links with other European Networks in relevant areas and disseminate project results to an extended audience across Europe.

THE I-LEAD PRACTITIONER WORKSHOPS

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 hosted by the project's consortium members. The workshops present a unique opportunity for experts to work as a collective 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 Investigation - Rome*
- ✓ *Cocaine in Transit - Madrid*
- ✓ *Public Order - Poznan*
- ✓ *Digital Forensics - Lisbon*

The results of these workshops are documented in the following pages of this brochure. Following the review of the 2018 workshops, it was decided to develop scenarios based around the outputs of the workshops to assist industry in understanding the challenges faced by the operational officers. These scenarios are included within each section of the brochure.

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.

Scenario

You are an investigator working within the cybercrime team and you are responsible for investigations of cyber related fraud. This morning a new report of BEC or sometimes known as CEO fraud came in with high priority. An internationally well-known company, which has several branches worldwide, have lost €19 Million due to a cleverly engineered scam.

Scenario Background:

The scam begins on 8 November 2019, when the CEO of the company in the Netherlands receives an email from the CEO of the headquarters, based in France. In this email, France ask to transfer €800.000 for acquisition of a foreign corporation based in Dubai. France explicitly mention not to speak or communicate with anyone about it, because they want to keep the competition out of the door. "The transaction must remain strictly confidential."

The Dutch CEO and the financial director locates this foreign corporation via the internet, because they had a strange feeling about this. After a short internet search they conclude that everything that's been described so far seemed to be correct.

After several emails between the CEO's and the financial director, the Dutch receive a signed confirmation of the transfer assignment from France. The Dutch transfer the €800.000 to the account as stated in the confirmation.

On 13 November 2019, the Dutch financial director receives a second money transfer request. This time an amount of €2.5 million. The CEO of France explains, the last transferred amount was just a small percentage of the whole acquisition amount. The €2.5 million is the second tranche of amounts that will follow. The Dutch also transfer the €2.5 million.

Between 13 and 16 November 2019 E-mail correspondence between the French CEO, the Dutch Financial Director and CEO resulted in a third tranche of 30% being prepared by the Dutch financial director, while at the same time an application was made to the 'cash pool' of the Company's Group in France. On 20 November, 30% was transferred.

On 22 November 2019, the French CEO confirmed to the Dutch Financial Director that the full acquisition price had been received. He also indicated that an additional budget between €5 and €9 million would be needed for 'communication and development'. He finally indicated that a similar request as before would have to be submitted for cash pool funding. On instructions, €5,826,770 was subsequently paid.

On 26 November 2019 the French CEO informed the Dutch Financial Director that an additional payment had to be made. Later that day, the French CEO made this specific and announced that after a decision of the Dutch CEO €5,152,354 had to be transferred. As a result, once again money was withdrawn from the cash pool.

On 28 November 2019 the French CEO informed the Dutch financial director that he would ensure that the withdrawn amounts totalling €19,244,304 would be refunded the next day. On the same day, questions came from France about the amounts withdrawn from the cash pool. During a telephone consultation that same day, it became clear that the company had become the victim of a so-called CEO fraud.

The Requirement:

1. Be able to quickly obtain bank account details
2. Be able to identify foreign money mules (accounts)
3. Be able to identify the CEO fraudster(s) (e.g. be able to identify IP addresses, be able to obtain useful information of foreign service provider information)

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 administrational 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.

Scenario

A major route for trafficking cocaine into Europe from the Caribbean is via sea cargo, with the drugs being concealed in shipping containers amongst various legitimate shipments. The drugs are often unloaded during transit onto smaller boats out at sea, and brought ashore into Europe at unmonitored locations, or they remain in the containers, reaching their points of destinations at ports throughout Europe, with the shipments then being collected by persons using various means.

The seizures of drugs by Law Enforcement in many cases are as a result of intelligence led investigations, or through detection of drugs using a range of techniques.

However, criminal gangs are becoming more sophisticated in their drug trafficking activities using technological solutions to cover their tracks, such as encrypted communication devices. They are also becoming more innovative in ways of concealment and becoming better at understanding counter surveillance methodologies.

Scenario 1
Background:

Intelligence has been received that a shipment of cocaine will be taken by vehicle to the point of embarkation and during transit within the Atlantic, be transferred from the container ship to a small craft for the remainder of the journey into Europe. During the intelligence gathering phase it transpires that the criminals are using end to end encrypted communications and are aware of surveillance methods used by the police.

The Requirement:

To gather information that can provide additional intelligence in relation to the transit of the cocaine shipment from its source to its destination and will:

1. Identify those involved in the trafficking
2. Gather information that would otherwise would not have been available through current technical means
3. Real time monitoring of the trafficking route

Solutions should be able to:

a. Enable encrypted communications to be intercepted in real time
b. Enable the electronic systems in vehicles to be interrogated
c. Enhance current audio capability reducing background interference

Scenario 2
Background

Intelligence has been received that there is a large shipment of cocaine being transported by container and will be offloaded at a port in Europe. The cocaine is concealed within the containers amongst legitimate goods.

The Requirement:

To locate the illicit goods being transported in shipping containers through:

1. Rapid screening
2. Targeted interventions using advanced intelligence analysis

Solutions should be able to:

a. Locate drug shipments through improved automated screening technologies

b. Enhance current search techniques utilising electronic detection methods
c. Provide real time in field analysis of substances
d. Improve screening intelligence to identify potential target containers

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.

Scenario

You are a police officer with a responsibility of maintaining public order during major events. You are preparing for a tournament final football match in your city, with neither of the competing teams being from your own country. Due to the importance of the match you are expecting a larger than usual number of fans, due to the fact that both teams are famous for having a large fanbase, that travel to the hosting country. Within both sets of supporters, there are groups who have a history and a reputation for inciting violence and have instigated violence against the police and property.

The official ticket allocation for each team is 5,000 but the game will be held in the national stadium which has a capacity of 49,000. You therefore expect that more than 5,000 supporters from each country will attend the match by attaining tickets either via the black market or via business or social connections. Due to this there is a high potential that opposing fans will be in close proximity of each other within the stadium, and additionally you will not know in which sections they will be.

Scenario 1

Background

You receive intelligence from one of the country's police force that supporters, who are thought to be connected to previous football hooligan incidents have booked flights to your city and are planning to travel a couple of days before the match. No such intelligence has come from the police from the other country, however the railway system across Europe means that it is easy for these supporters to buy train tickets at short notice and avoid the eye of the police intelligence gathering services.

The Requirement

1. To identify, track and monitor those persons of interest that you

have already received intelligence on as soon as they arrive in your country and their subsequent movements

2. Be able to communicate with all supporters in real time when they arrive in your country, to ensure they are kept updated about the event including; routes to the stadium, 'no-go' areas, what to do in an emergency, who to contact if they feel threatened etc.

Scenario 2
Background

Both sets of supporters have, in the past, had known links with infamous hooligan firms which have gained notoriety in certain circles around Europe. An attack from either of the teams supporting fans could be seen as prestigious and a way of gaining respect from hooligans or ultras groups within your own country. There are rumors of such an attack on social media and you are required to plan the response to this which will include interaction with fans prior to any operational responses whilst minimising the risks to the public and property. Direct confrontation with fans is a last resort, however, consideration must be given to the use of tactics, technology, vehicles and protective equipment in order to successfully manage any escalations.

The Requirement

1. Be able to identify quickly, any changes that occur in the pattern of crowd behavior that indicates a potential violent surge
2. To consider how to improve and speed up the real time decision making and tasking process
3. Be able to deploy resources and equipment to a potential incident to de-escalate and diffuse the situation.
4. To consider how current protective equipment for police officers can be improved

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.

Scenario

An organised crime group are suspected of trafficking drugs and humans across various European countries and intelligence suggests that they also have links to South American drugs suppliers. The network is operating across different European and wider international boundaries and are using end to end

encrypted messaging services to communicate. Their commodities are offered for sale over the dark web with payments being made using virtual currencies as well as direct cash payments when trafficking humans between various countries. The OCG operate across a complex network maximising the use of technology to carry out their illegal activities.

Scenario Background:

As a result of a number of intelligence led operations, a number of electronic devices have been recovered from suspects believed to be involved in the importation and subsequent sales of illegal drugs. The devices are password protected and the law enforcement agency is unable to access the information held on the device that may provide valuable information relating to the operations of the OCG. The devices have significant capacity to host secure data including images and videos. At least one of the devices has been deliberately damaged in an attempt to prevent the device being accessed and subsequent destruction of information held upon the unit. It is anticipated that the devices will provide access to large volumes of information held locally on the device, linked devices and also via cloud based storage. Current commercial tools are not in a position to access passwords due to the relatively inadequate dictionary libraries in use nor are they able to provide an effective triage of the volumes of data held.

The Requirement:

To unlock the devices in order to access information that may be held on the device or lead to other sources that can provide evidence and intelligence in relation to the importation and sales of illegal drugs and will:

1. Identify those involved in the activities
2. Gather information that would otherwise would not have been available through current technical means
3. Increase the speed of extraction and analysis
4. Repair damaged devices to enable effective extraction of data

Solutions should be able to:

a. Provide an effective and timely solution to password cracking of secure devices
b. Adopt a 'less manual' method for the extraction of information and its subsequent analysis
c. Improve triage of complex data sets
d. Integrate existing commercial tools to provide correlated results
e. Develop a means to identify and transplant damaged component parts that will bring devices 'back to life'

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 regard to encryption of devices and password cracking. Password cracking 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*

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 opensource, 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 smarter capability would enhance the way large amounts of data are 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 differentiate between relevant and non-relevant data 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 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 building upon existing capability (ECTEG) to develop 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 a factor was the discipline not having a framework of learning and ongoing standards of competency alongside bureaucracy and workload. Additionally, highly knowledgeable staff were leaving digital forensics as their expertise could earn them more money in other business sectors. With regard to 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 regard to 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 cons 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. The current EPE platform was not considered to be user friendly and a method of dissemination and communication was essential..

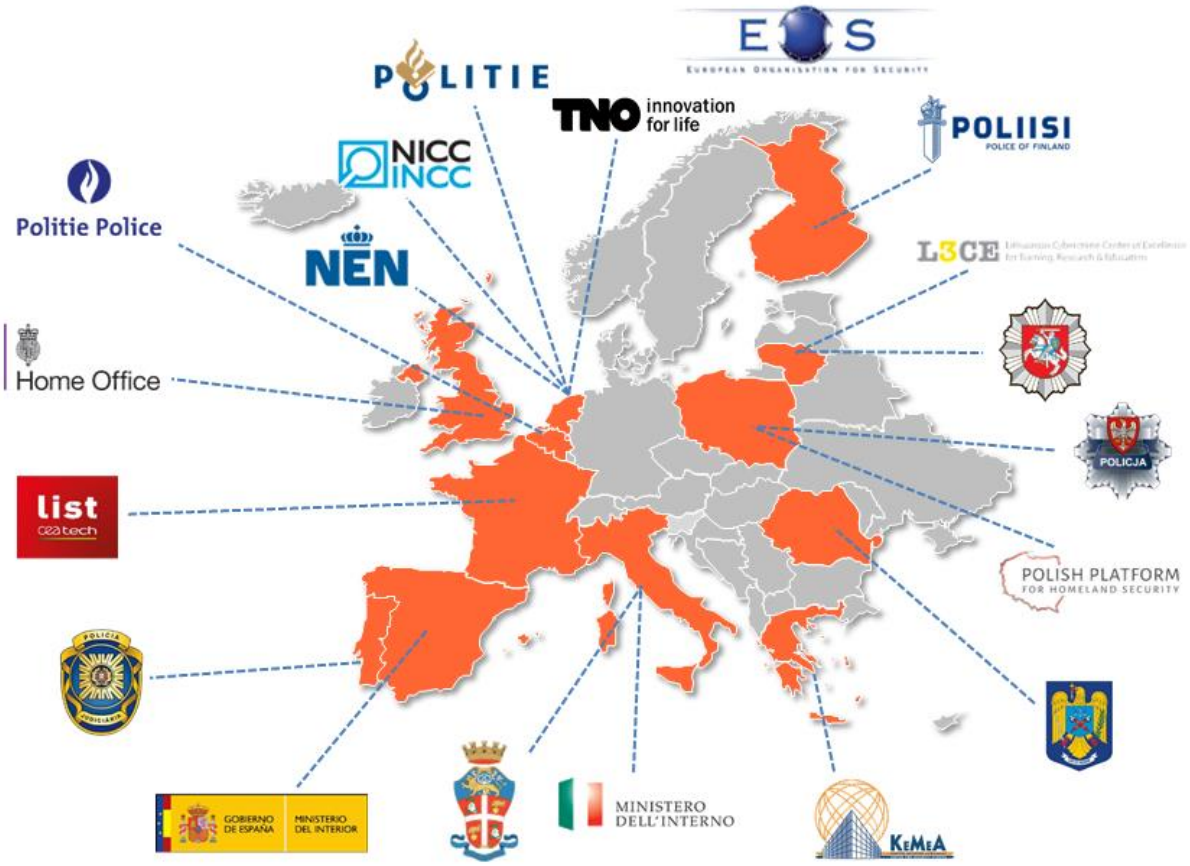
2020 Practitioner Workshops

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. The subjects covered are shown in the table below;

Subject	Hosting Country	Month
Forensic Crime Scene Recording	**Belgium**	**March**
Digital Investigations	**Lithuania**	**April**
Firearms Trafficking	**Czech Republic**	**June**
Cyber Extortion (TBC)	**Greece**	**September**
Vehicle Mitigation	**Finland**	**November**

i-LEAD

innovation - law enforcement agency's dialogue



www.i-lead.eu

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