POLIIICE

Newsletter

Issue #1 - April 2023

POLIIICE - Powerful Lawful Interception, Investigation, and Intelligence

Editorial by BayHfoD (Coordinator)

POLIIICE vision is to advance European LEAs to a novel lawful-interception (LI), investigation and intelligence era in which they will be able to effectively prevent, detect and investigate crime and terrorism amid the new age of communication (5G&Beyond, end-to-end encrypted communication and Quantum based encryption). These new age technologies turn legacy LI solutions to totally in-effective and therefore put significant risk on Europe's fight against crime and terrorism.

POLIIICE will offer, research, validate and demonstrate array of innovative LI measures at cloud & network level as well as at edge device level that together will enable LEAs to efficiently overcome the new age challenges and enable high throughput of its LI.

In addition, POLIIICE will research and model QUDDaaS (Quantum unlock, detection and decryption as a service) as an envisaged central service, potentially outsourced at pan EU level, which will harness quantum computing for decryption of lawfully intercepted encrypted communication (which is vulnerable to Quantum's Shor algorithm), for brute force detection of target-user's credentials/tokens needed to access encrypted cloud-native apps and for Quantum unlock of lawfully seized edge devices. QUDDaaS may also detect and classify LI communications that are resistant to Quantum decryption power and therefore can't be decrypted. POLIIICE also aims to improve the information exchange and cooperation among European LEAs by proposing and implementing a mechanism and procedure for exchanging pseudo-anonymized suspect identifiers. POLIIICE is designed for ensuring the cost-effectiveness, security and integrity of the new age LI and will provide the legal and ethical framework for each of its measures while strictly complying with privacy preserving and ethics rules of operation. POLIIICE will contribute to the LI standardization and will recommend EU regulation changes for effective adaptation of POLIIICE vision and innovative LI measures.

The significance of the POLIIICE solution lies to the fact that it is the first time that research funds are awarded to such an important security research effort on behalf of the EC, within the framework of prevention and fight against Organised Crime and Terrorism.

Despite the fact that POLIIICE project runs only for a few months, the Coordinating Team in collaboration with Consortium partners have already presented the POLIIICE solution to EU Institution such as Europol, EC3 as well as international Institution such as the Security Committee of the UN, attracting the interest of their audiences.

The involvement of important Government authorities, major research institutions of the EU Member States and large scale business companies, showcases that the Innovation Roadmap as it is strategically schemed by the EC, will contribute to the utmost degree to the necessary synergies for the Market Uptake. Synergies which clearly find as the ultimate beneficiaries the EU Citizens assuring their everyday life security.

POLIIICE Project is the tangible effort towards our Innovation Union, our Security Union.

LI in the New Age of Communication

The new age of communication technologies which include 5G networks and E2EE applications like WhatsApp, Signal, Telegram, Slack, Kik, Gmail and others, as well as the emergence of Quantum technologies are critical building blocks of our digital economy and society[1]. Despite the many anticipated benefits of these new age of technologies, from LEAs perspective they createe number of challenges pertaining mainly to the ability of LEAs officials to effectively carry out effective lawful interception (LI) which is crucial for the fight against crime and terrorism and for keeping our societies safe and secure.

LI in the new age of communication should be broad in scope in order to be effective. Nevertheless, until less than a decade ago, before the emerging of E2EE communication applications it was quite narrow and limited to two main measures:

Compliance LI- the legal compliance of CSPs (Communication Service Providers) to provide LEAs standardized interfaces for LI.

Tactical LI- LI and location tracking done, over the air interface, in the vicinity of the targets, using IMSI catchers (also known as 'Stingray LI').

These two measures used to give LEAs full visibility of the lawfully intercepted communication and satisfied their LI requirements. At that time ('the legacy LI era'), all the communication channels, including their encryption (if any) were fully controlled and managed by the CSPs as all the communication went through their networks and not on top of their networks (as it is with WhatsApp, Signal, Telegram, Gmail etc.), and if it was encrypted the CSPs were able to provide the decryption keys to the LEAs' officials. So, LI was relatively easy and fully dependent only on CSPs and LEAs.

However, a new era of LI began few years ago when first E2EE communication applications were launched and started to gain traction (Telegram was launched in 2013 and WhatsApp became full end-to-end encrypted in May 2016[2]). It was a new reality, in which the encrypted communication applications were totally out the CSPs and LEAs control and the above two legacy LI measures, could not provide the requested lawfully intercepted communication content (CC) for such encrypted communication apps.

To overcome this severe disability, LEAs had to approach directly with a warrant to the communication apps providers (possible only if the app provider is based in the same country of the LEA or at the EU for EU member states and many times it is non-effective because of the end-to-end encryption) and more importantly, LEAs had to consider very seriously adding new measures to their LI portfolio, such as:

Classification of encrypted lawfully intercepted communication based on metadata analysis (usually metadata is kept unencrypted) or DPI (Deep Packet Inspection). The classification means to detect the communication app used (WhatsApp, Telegram etc.), the identifiers of the terminals creating the communication (IMSI/MSISDN/Email address etc.) and the content type (text, audio, image or video).

Forensic extraction of data from these cloud native applications by using (and unlocking) lawfully seized edge-devices using forensic unlock and extraction COTS products.

Variety of Cyber Intelligence measures.

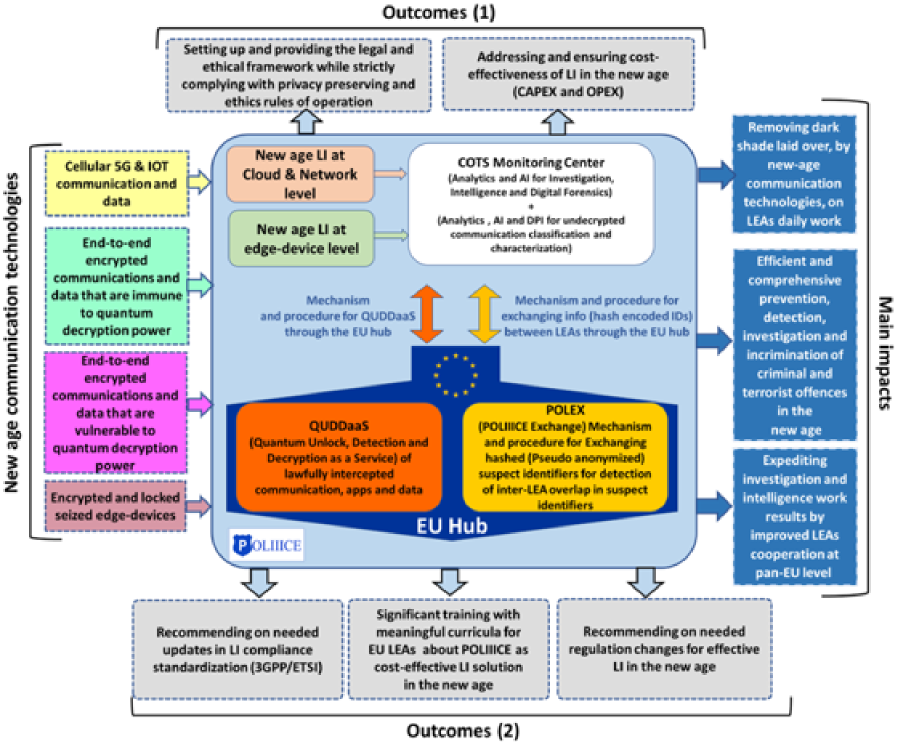
Interfaces to mobile-ad network companies.

These new measures have joined to the above two measures, changing the scope of LI from narrow to broad and quite complex. In other words, LI became broad and complex in scope even before the emergence of 5G networks and Quantum technologies. Nevertheless, 5G and Quantum significantly intensify the complexity of LI in the new age by adding their inherent challenges to the LI.

Some of the 5G challenges are its cloud (virtualized) architecture and network slicing which may include network elements and service providers outside the jurisdiction region of the intercepting LEA, Multi-access edge computing (MEC) of 5G technology, the tremendous data volumes expected per intercepted 5G target, concealed identifiers over the 5G air interface and 5G base stations authentication (done by the 5G core network) which challenges the Tactical (off-air) LI of 5G edge devices performed by IMSI catchers and some of the Quantum challenges are the risk that Quantum based encryption and quantum based networks might be abused by terrorists and criminals to evade LI as it they are fully resistant to any brute force attacks even if they are conducted by Quantum computer empowered by Shor's algorithm and the fact that Quantum computers today are still not commercial and once they will be commercial, they probably will be very expensive, so it will be financially difficult for LEAs to afford them in order to expedite investigation and intelligence work.

Nevertheless, 5G and Quantum computing also bring some opportunities to LEAs. 5G localization of targets will be more accurate than in 4G and 3G because of the higher granularity of the 5G radio and higher density of 5G base stations and it will allow to gather rich evidence from IOT devices. In addition, Quantum computer that runs Shor's algorithm will be able to decrypt very quickly and efficiently, traditional public key E2EE communication (used today by many of the above cloud native apps like WhatsApp, Telegram and similar) so LEAs will get high throughput of LI from E2EE communication which means less dependency on other more legally sensitive (and expensive) measures and edge device dependent measures such as Cyber Intelligence. In addition, Quantum computation power can be used for brute force unlock of lawfully seized edge devices and cloud native apps (by detecting Password, PIN or Token using Grover's algorithm) in order to extract their data to enrich the LI and expedite the investigation and intelligence work.

To summarize, effective LI in the new age should be based on multiple LI measures that only when combined together, will enable LEAs the high LI throughput needed to overcome the new age challenges. Following these challenges also the CSPs' compliance LI will have to evolve to support 5G and overcome new emerging challenges by supporting new measures that should be standardized like new interfaces to support Cyber Intelligence, IMSI catchers of the new age, LI from mobile-ad networks, Quantum resources and more.


Outcomes (1)
Setting up and providing the legal and ethical framework while strictly complying with privacy preserving and ethics rules of operation
Addressing and ensuring cost-effectiveness of LI in the new age (CAPEX and OPEX)
New age communication technologies
Cellular 5G & IOT communication and data
End-to-end encrypted communications and data that are immune to quantum decryption power
End-to-end encrypted communications and data that are vulnerable to quantum decryption power
Encrypted and locked seized edge-devices
New age LI at Cloud & Network level
New age LI at edge-device level
COTS Monitoring Center
(Analytics and AI for Investigation, Intelligence and Digital Forensics)
+
(Analytics , AI and DPI for undecrypted communication classification and characterization)
Mechanism and procedure for QUDDaaS through the EU hub
Mechanism and procedure for exchanging info (hash encoded IDs) between LEAs through the EU hub
QUDDaaS
(Quantum Unlock, Detection and Decryption as a Service) of lawfully intercepted communication, apps and data
POLEX
(POLIIICE Exchange) Mechanism and procedure for Exchanging hashed (Pseudo anonymized) suspect identifiers for detection of inter-LEA overlap in suspect identifiers
EU Hub
POLIIICE
Removing dark shade laid over, by new-age communication technologies, on LEAs daily work
Efficient and comprehensive prevention, detection, investigation and incrimination of criminal and terrorist offences in the new age
Expediting investigation and intelligence work results by improved LEAs cooperation at pan-EU level
Main impacts
Recommending on needed updates in LI compliance standardization (3GPP/ETSI)
Significant training with meaningful curricula for EU LEAs about POLIIICE as cost-effective LI solution in the new age
Recommending on needed regulation changes for effective LI in the new age
Outcomes (2)

This means that LI regulations (legal framework), LI standards (provided by standardization bodies like ETSI/3GPP), CSPs and potentially Mobile-Ad networks companies will have to adapt accordingly while the LI measures in the new age will continue to develop and grow with the fast pacing and dynamic nature of the new communication and quantum technologies.

[1] Council of the European Union. "Position paper on 5G by Europol" (Council doc. 8268/19). Brussels, April 11, 2019.

[2] "WhatsApp Introduces End-to-End Encryption". The New York Times. April 5, 2016.

POLIIICE in Third Intersessional Consultation of the Ad Hoc Committee

The Third Intersessional Consultation of the Ad Hoc Committee was held on November 3rd and 4th, 2022, in Vienna, Austria, bringing together experts from various sectors to discuss the use of information and communication technologies (ICTs) for criminal purposes. The meeting aimed to elaborate a comprehensive international convention on countering cybercrime and to provide a platform for experts to exchange their experiences and ideas.

Mr. Farhan Sahito, Director General at Privanova SAS, who is a leading provider of privacy and risk management solutions with a focus on the GDPR, participated in Panel 4, titled "A Concerted Effort: The Role of the Private Sector in the Fight against the Use of Information and Communications Technologies for Criminal Purposes." The panel brought together top industry leaders, including Ms. Pei Ling Lee, Head of Cyber Capabilities and Cyber Strategy at INTERPOL, Mr. Nemanja Malisevic, Director of Digital Diplomacy at Microsoft, and Mr. Will Hudson, Corporate Counsel at Google Inc., on behalf of the International Chamber of Commerce-United Kingdom, and Ms. Megan Stifel and Ms. Zoe Brummer, Chief Strategy Officer and Principal Coordinator of the Framework for Cyber Incident Reporting respectively, on behalf of the Institute for Security and Technology.

Mr. Farhan Sahito represented the project POLIIICE and presented the main aims and objectives of the project, alongside other EU-funded projects, CYBERSPACE, CC-DRIVER, and TRACE, to inform UN Member States of the ongoing and upcoming work in tackling cybercrime and supporting law enforcement agencies.

He emphasized the increasing volumes of cyber-attacks and the limited resources and capabilities of law enforcement authorities to tackle them, underscoring the importance of strong public-private partnerships in the fight against cybercrime.

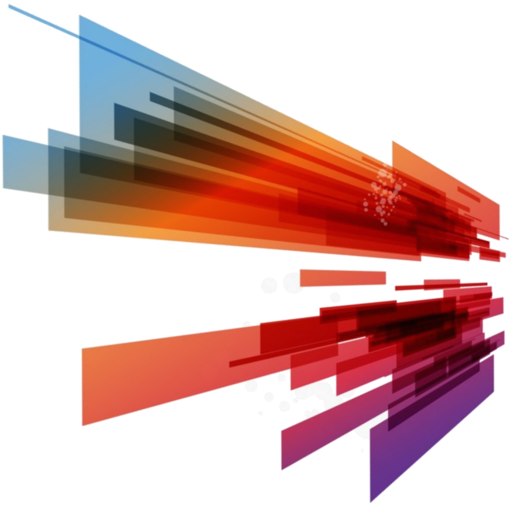
Mr. Farhan Sahito also briefed the meeting on the reasons for underreporting of cybercrime in the private sector, including lack of resources and perceived negative consequences for businesses. He emphasized that regulatory frameworks play a crucial role in fostering public-private partnerships and that a balance between penalties and incentives for private sector companies should be struck, while considering their needs. This will stimulate and facilitate the reporting of cybercrime by private sector companies, enabling law enforcement authorities to take necessary actions and prevent further attacks.

In conclusion, the Third Intersessional Consultation was a valuable platform for experts to exchange their experiences and ideas on countering the use of ICTs for criminal purposes. Mr. Farhan Sahito's presentation, along with the presentations of other industry leaders, highlighted the critical role of the private sector in the fight against cybercrime and the need for a comprehensive and balanced approach to tackle this growing problem. The meeting in Vienna served as a starting point for further discussions and actions towards a safer and more secure online environment.

United Nations

Office on Drugs and Crime

POLIIICE



POLIIICE 1st Workshop in Paris

Paris in France was chosen in march 2023 by the POLIIICE european consortium to host the 1st Workshop on the needs of the LEAs, Law Enforcement Agencies, in the field of the future evolutions of the legal interceptions.

The french home ministry with the DMIA organised with PRIVANOVA two days of workshops in the LUMIERE building of the center of Paris. First, we took the time of a dinner to create in 2023 a direct discussion among the consortium delegations to discover each other in another way, as the multiple visioconferences that took place since the Munich's meeting of october 2022. The french « Creole » cuisine of the Reunion island located in the Indian Ocean was shared in order to mark our gratitude to the fifty researchers, police officers, industrial experts and decision makers that came together.

Hard work was done on the second day in Paris from 8am to 7pm by all the participants sharing their knowledge on legal interception futur needs and solutions. The Estonian Police and the DMIA gave a complete presentation of the first results of a questionnaire that had been elaborated by the WP 1 members. With 16 to 20 questions, the POLIIICE study interested more than 105 police forces working in 14 European countries. The results show, in 2023, how difficult it is to fight against criminal organisations because of their massive use of encrypted systems provided by compagnies located inside or outside of Europe. A study will be produced and delivered in the last days of may 2023.

When a criminal organisation can use Whatsapp or Telegram easily and grow its activities with the help of encryption, the work of a LEA is heavily impacted. Protecting the citizens and the public institutions, as well as defending our private compagnies is more and more complicated in the new 5G world where the criminal and terrorists organisation can have permanent discussions between their members. The future situation can be considered as difficult or even alarming with the reduction of this LI tools for the efficiency of the vast majority of LEAs in Europe. Drug dealers, human trafficing and terrorists are using encryption massively.

The criminal organisations could increase their capacities to grow if the police forces are not able to destroy quickly their modification of size. Small criminal organisations get bigger when they are able by the encryption of their communication systems, to manage easily their ressources and work with lawers or digital engeneers. Encryption in 2023 is a service provided massively to those criminal organisations and this situation is completely new compared to what happened from the 1995 to 2020 era where they had access to mobile phone systems, but without massive encryption systems. The LEAs could do a good job in the past by listening to the phone communications of drug dealers, terrorists and child pedopornograffic dealers. They could, with the legal interceptions realize under the control of the judges, a destruction of those criminal organizations. Now, it is much more complicated and the situation needs new measures and technical capacities to come back to the previous situation.

Bringing together, with the help of the Bavarian Police School of Germany and the Estonian Police, more than 50 researchers, telecom experts and handusers of the security forces, gives a new capacity to POLIIICE to work with more efficience to find the legal and the technical answers. Bulgaria and Switzerland participated for the first time to a part of the POLIIICE research program bringing a contribution of the analysis.

The telecoms, research or industrial actors with for instance the CEA, TELEFONICA, NOKIA, CHAPSVISION, RHODE & SCHWARZ or CENTRIC and BAE SYSTEMS shared impressive analysis that might be very useful for the future research done by the POLIIICE consortium. The political deciders at national and European level will benefit of this resarch teams to have a precise view of what happens in the field of legal interceptions. This can give in the next years tools to help to build a better legislation against criminal organisations use of encrypted systems. The police forces can hope to get new capacities to avoid a catastrophic situation in the coming years if we leave a complete free use of encryption, with low-costs benefiting all the criminal organisations that want to expand their activities in Europe.

The DMIA was proud to host this productive Paris POLIIICE seminary, which was so useful to our researchs. The workshop was a success and we hope that every member of the consortium is satisfied with it.

POLIIICE

Coordinator

Hochschule für den
öffentlichen Dienst
in Bayern

Fachbereich
Polizei

Project Partners

DMIA

POLICJA MAZOWSZE

LibereU
A boutique SME for co-creation of innovation

ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ

Privanova
Research & Consulting

Polisen
Swedish Police

POLITÉCNICA

MUNI

KEMEA

cea

Telefónica

NOKIA

ROHDE&SCHWARZ
Make ideas real

Estonian Police and Border Guard Board

ELEKTRON
by FLANDRIN TECHNOLOGIES

KPMG

CENTRIC
Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research

BAE SYSTEMS

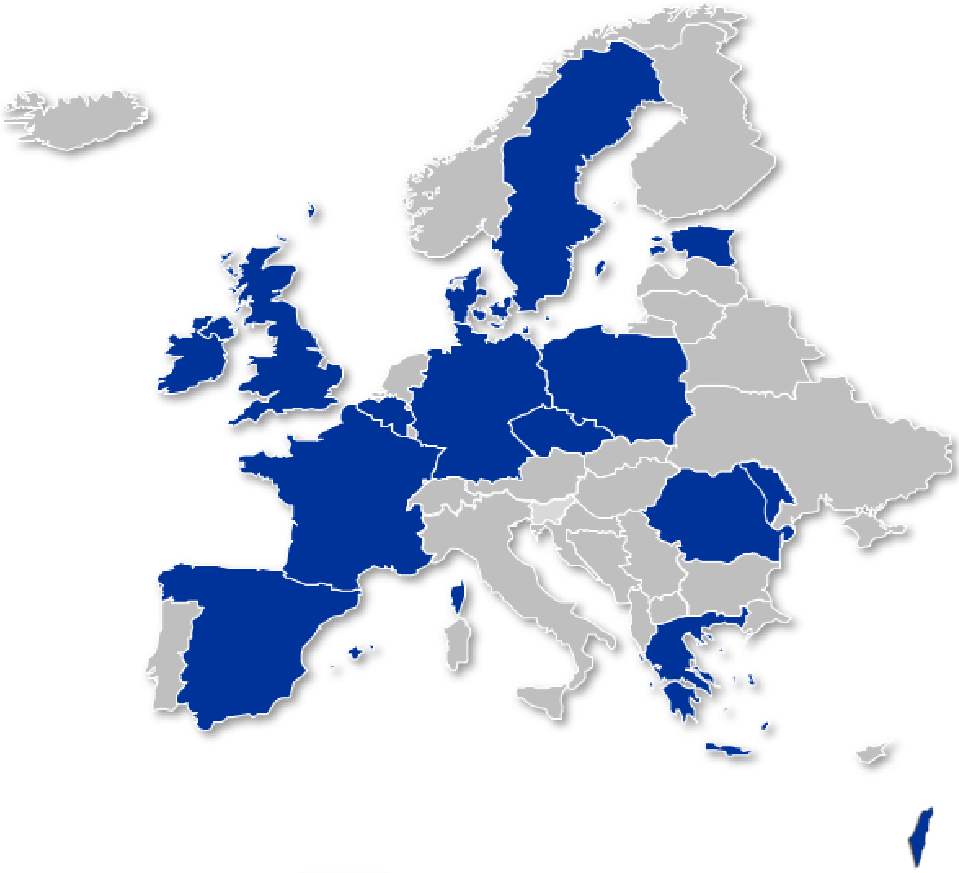
https://www.poliiice-project.eu

website

LinkedIn

Twitter

Instagram



POLIIICE Project has received funding by the European Union's Horizon – Research and Innovation Framework Programme, under grant agreement no 101073795