# Early Pursuit against Organized Crime Using Environmental Scanning, the Law and Intelligence Systems:

The ePOOLICE Project (Early Pursuit against Organized Crime Using Environmental Scanning, the Law and IntelligenCE Systems) project is funded by the European Commission under the Seventh Framework Programme for Research and Technological Development (FP7). The list of partners working on the project alongside UNICRI includes law enforcement officials and academic experts specialized in matters of organized crime and criminal networks. The environmental scanning systems will operate by drawing on a repository of all relevant information and knowledge, including scanned information and derived, learned or hypothesized knowledge, as well as the metadata needed for credibility and confidence assessment, traceability, and privacy protection management.

Organized crime is becoming more diverse in its activities and methods including “greater levels of collaboration between criminal groups, greater mobility in and around the EU, a diversification of illicit activity, and a growing dependence on a dynamic infrastructure, anchored in key locations and facilitated by widespread use of the Internet” (the Director of Europol, in his foreword to the OCTA 2011 report). An important means for law enforcement in combatting such crime is strategic early warning which is heavily depending on an efficient and effective environmental scanning.

For this, the ePOOLICE project will—in close collaboration with law enforcement partners, as well as criminological and legal experts—develop a prototype of an environmental scanning system implementing solutions applying the most promising technological advances and breakthroughs as provided by the RTD partners. The solutions will be tested and evaluated through running realistic use case scenarios that are developed by our user partners.

Central to the solution is development of an environmental knowledge repository of all relevant information and knowledge, including scanned information and derived, learned or hypothesized knowledge, as well as the metadata needed for credibility and confidence assessment, traceability, and privacy protection management. For effective and efficient utilization, as well as for interoperability, the repository will apply a standard representation form for all information and knowledge.

For effective and efficient scanning of the raw information sources, the project will develop intelligent environmental radar that will utilize the knowledge repository for focusing the scanning. A key part of this process is semantic filtering for identification of data items that constitutes weak signals of emerging organized crime threats, exploiting fully the concept of crime hubs, crime indicators, and facilitating factors, as understood by our user partners.

# OBJECTIVES:

The overall aim of the project is to create an international environmental scanning system dedicated to countering criminal networks. The development of the platform will be guided by the end-user needs and the ethical/legal issues through active participations of LEAs and application of use case scenarios providing a problem oriented drive for the project and using privacy by design approach. As depicted in the attached figure , “The ePOOLICE system “, a key component of the framework is semantic filtering for identification of data items that constitutes weak signals of emerging organized crime threats, exploiting fully the concept of crime hubs, crime indicators, and facilitating factors, as understood by our user partners.

The main objectives of the project are solutions supporting:

**1**. Detection of organized crime:

1. Detect the existence of criminal activities typically run by organized crime.
2. Discover organized crime and underlying criminal organizations as early as possible to prevent further formation of stronger, more resilient criminal systems.

**2.** Prediction of the evolution of organized crime. This requires environmental scanning system for analyzing and developing scenarios of possible threats in the future.

The ePOOLICE environmental scanning system will provide a systematic overview of the surrounding environment to better appreciate, assess and anticipate an emerging crime, by monitoring the environment and capturing in real-time relevant information present in heterogeneous sources, including law enforcement analysis reports, governmental information, web, social media, news, academia, non-governmental and international organizations, and subject matter experts.

# Specifically, the system will support:

* Disparate information sources and diverse media forms (free text, audio);
* Multiply lingual support, with English and German implemented;
* Dissemination and exchange of information and knowledge of potential interest to the law enforcement agencies;
* Visualization of potentially emerging OC threats for OC threat assessment;
* Early warning with alerts in cases of detection of potentially emerging new OC threats;
* Storing and utilization of hypothesis and notes from user;
* Utilization of user feedback on findings for refinement of the system’s domain knowledge; analysis and decision making in addressing emerging OC threats, considering the validity and the seriousness of the detected threats.

# System Architecture:

Three of the key components of ePOOLICE's technical architecture are the environmental knowledge repository (EKR), data fusion and analysis tools (further analysis). These components are then integrated and represented using a number of visualization tools displaying threat indicators geographically along with subsidiary information such as trends and meta-data detailing the source and validity of indicators; information that can be applied by decision makers.

# Situation Assessment:

One aspect of ePOOLICE’s analytical armory is Formal Concept Analysis (FCA), a semantic data analysis method that captures, categorizes and delivers data meaning in real time to influence decision makers through ontologically modeling the relationships between objects and their attributes [15]. FCA presents the sources of organized crime indicators as formal objects. These sources may be made up of Tweets, web pages and police reports. The indicators themselves are presented as formal attributes, with attributes forming the characteristics of objects. Attributes are made up of named entities such as the identification of location, time and organized crime gang, thus enabling situation assessment. As a result, formal concepts represent frequent groups of indicators along with situation assessment information. The more frequent the group, the more weight can be given to the evidence. Situation assessment allows information to be appropriately visualized depending on the requirements of the analyst. For example, a map-based system to represent threat indicators geo-graphically may form the basis of one such approach to visualization. This can also include a measure displaying the frequency level itself, giving the analyst control over the levels of support that they are interested in. In FCA, the scaling of continuous attributes, such as geospatial (see Figure 3) and temporal values gives the analyst control over situation assessment. Applying a 'zoom' like functionality allows the analyst to see a more aggregated, strategic perspective when 'zoomed out', while 'zooming in' enables the focus to be concentrated on individual events or sources. In temporal terms, ‘zooming out' gives a more strategic, historical view of events, with 'zooming in' focusing solely on the current situation.

# Security Perspective:

In a security perspective, the system functions as a tool for strategic intelligence led activities focusing on modus operandi, hotspot locations, emerging crime patterns and (mega-) trends lurking in the horizon. For that reason, personal data are not relevant in the information context of ePOOLICE, since the system does not aim at identifying individuals. Hence, the use context of ePOOLICE is situated at the strategic level, implying that the system does not support the operational level (such as for instance prosecution, forensic) at all. As such, ePOOLICE serves a pure preventive purpose in scaffolding sense-making activities carried out by law enforcement agents and analysts engaged in countering threats and acting proactively in dealing with future upcoming crime scenarios and trends in organized crime. A privacy preserving design framework is under development in the system development process in order to address issues of anonymization of potential personal and or sensitive data. Moreover, other privacy safeguards, regarding system functionalities, have to be addressed as well, such as for instance considerations to permit management of different user-levels of authorization. In that respect, logging of system access and processes might ensure tracking of possible unauthorized use of data and further support control procedures by internal data controllers as well as by independent authorities.

As such in seeking to balance data privacy and data utility, the design of ePOOLICE takes departure in a privacy preserving system development approach supported by legal research (De Marco, 2009, 2014) and in compliance with EU data protection law. But, the increase in technology led policing initiatives also calls for a broader discussion of the impact of security technology systems, such as ePOOLICE, at a societal level, a discussion, in which this article sets out to address issues related to the balancing of privacy and national or public security.

# Balancing national security and citizens' right to privacy:

The concept of security is not easily defined but can be conceived of as dealing with wellbeing at state level and protection of democratic institutions. Over time, the classical state-oriented notion of security has changed towards a more individual-centered approach, emphasizing the integrity and security of the individual and protection from threats (Liotta, 2002). The rise of a human security framework as necessary for individual as well as national and global security is reflected in the United Nations' Human Security Doctrine (2003) and in the Human security doctrine for Europe (2004). Within this framework, security can be defined as nonattendance of danger at a state level as well as at a societal level with reference to the citizens forming the society. Moreover, the EU Security Strategy (2004) emphasizes the need to act proactively in dealing with key security threats (Raguse et al, 2008,p.16 ff.). As such, prevention is the core goal of EU security policy implying a proactive stance towards unclear risks and threats, which stem from terrorism, organized crime, environmental disasters and diseases. Hence in order to act proactively and predict future outcomes, one has to be able to reveal patterns of information in complex dynamic changing environments, and for that reason data veillance has become a central component in modern security policy. From this viewpoint, we are faced with the challenge of striking a balance between two sides of security; formulated as absence of organized crime threat s and preservation of the freedom and integrity of citizens as important preconditions for a flourishing democracy.

Issues of security and surveillance of citizens are frequently framed as a dichotomous clash between citizens' right to privacy as opposed to national security, implying a zero sum game in which more security is necessarily followed by less privacy. This observation may give raise to civil society concerns regarding privacy rights in ePOOLICE. But given that security is also an intrinsic value for human well-being at a fundamental level, we might move beyond the dichotomy between citizens' right to privacy and national security and instead conceptualize security in terms of interacting and mutual dependent dimensions of security; i.e. as individual security and public and or national security.

From a public point of view, an example of European citizens' opinion on privacy and security issues can be found in a participatory technology assessment which concludes that citizens are open to legitimate security measures for crime prevention, whereas reference to terror treats does not justify privacy limitations for most citizens, probably due to the fact that very few citizens have actually been exposed directly or indirectly to terror, whereas most people have been affected by crime one way or the other. Consequently, it seems to be the case that people are prepared to value security over legitimate restrictions of privacy in specific contexts reflecting individual dimensions of security.

To elaborate on this from a legal perspective; any limitation to fundamental rights of privacy and personal data protection has to respect some basic principles in order to be legitimate and ensure that privacy is not violated. Consequently, limitations have to rest on a legal basis and must be formulated with such a degree of precision that it enables citizens to understand how their navigation and conduct in society are affected by the given limitations. Moreover, a restriction must pursue a legitimate aim, i.e., be in accordance with listed legitimate aims, formulated within each article of rights in the European Convention on the Protection of Human Right and Fundamental Freedoms (ECHR) as aims that justify interference. Furthermore, any limitation must correspond to a real need of society and must be seen as an efficient instrument (for instance in relation to crime reduction and security). Finally, the principle of proportionality seeks to guarantee that the limitation is balanced to the aim pursued. In order to minimize the infringement of privacy rights and to assess the proportionality of a restriction, important issues to settle are whether the overall effect of the constraint is reasonable and whether it is the least intrusive mean available Here,to ensure that privacy is not violated, the ePOOLICE project must specifically see if the requirements of necessity and proportionality of a potential privacy restriction is satisfied and if the system is based on an appropriate legal basis. Given these circumstances, the ePOOLICE project strives to enhance both privacy and security by introducing pro-active privacy enhancing design principles throughout all stages of the development process - for instance by carrying out privacy impact assessments specifically targeting the challenges inherent to the development of the ePOOLICE system In this way, the project seeks to develop technological solutions that support privacy compliant use.

Privacy is usually regarded as an instrumental value, but of a special kind since it is also a necessary condition for the fulfillment of important human goals, i.e. intrinsic goods, such as autonomy, friendships and the formation of social relations. Consequently, in our technology mediated context, particularly attention is paid to informational privacy) as individuals' ability to control the flow of personal information, including how information about them is exchanged and transferred. Benn's argument below encapsulates the importance of privacy for autonomous decision making and for the formation of identity:

"The management of so complex a set of relations and the self -assessments and revisions implicit in it, would be quite impossible if one could not insulate one life-sector from another, if one could not choose what of oneself to reveal here, what there. One underpinning of privacy claims, then, is the interest a person has in establishing, sustaining, and developing a personality. Taken off his guard, discovered in one role while projecting the persona of another, a person is embarrassed because he has lost control of his personae in an ambiguous situation and is at a Joss to know what response is appropriate in terms of the complex notion he has of himself". (Benn, 1988, p. 282)

# Guiding Questions:

* What exactly is the aim of the ePoolice?
* How environmental scanning system can work to anticipate an emerging crime?
* How awareness about environmental scanning system among individuals can be raised?
* What are the tools needed for environmental scanning and data acquisition?
* How the security and law enforcement forces should form themselves to meet the emerging threats and crimes?
* What are the major forces that drive such kind of threats and crimes?
* Is the environmental scanning system interfering with citizen’s privacy?
* How an individual’s privacy and national security can be preserved while fighting Organized crime threats?
* What are the macro environmental factors that influence the emergence of threats and how they impact them?
* For the purposes of prototype system what does the OSINT (Open Source Intelligence) refers to?
* How does FCA (formal concept analysis) analyze the data and implicit relationships between objects?
* How Leas and other government authorities can prevent individuals from informational wrongdoing?