Europol’s Crime Analysis System – practical determinants of its success

Abstract:

Threats to modern nation states from organised crime and terrorism create environments in which intelligence becomes a vital component of policing and security plans but the increasing use of personal data for law enforcement purposes can alter the normative relationships between stakeholders and law enforcement agencies and between agencies and citizens. For that reason, police intelligence practice demands critical examination. This paper presents a narrative inquiry, based on the authors’ experiential knowledge and empirical research, into Europol’s Crime Analysis System (ECAS). The study explains Europol’s efforts to develop data collection and analysis systems that meet the needs of EU Member States. Through ECAS, it has created powerful tools intended to deliver intelligence products that help Member States identify, localise and neutralize transnational threats to a degree not witnessed before in Europe. Nevertheless, Europol’s performance in this context seems sub-optimal. Shortcomings largely are attributed to a lack of trust between Europol and Member States leading to failures to share information between themselves and with the institution. The result is that the latter’s strategic intelligence products sometimes are deficient or incomplete. That should be of concern to stakeholders because Europol’s strategic intelligence efforts may be rendered ineffective. Shortcomings in Europol’s intelligence products also are significant for citizens because they may mean that the information-sharing process is less transparent and less accountable than citizens have a right to expect.

***

Key words:

Europol; crime intelligence; trust; crime analysis; information-sharing.

Introduction

This paper presents a case study of the development of the crime intelligence system of the European Police Office, Europol. In modernity, threats to nation states from organised crime and terrorism create environments in which policymakers turn more readily to information-based instruments of control. Traditionally, the collection, analysis, and evaluation of crime intelligence have been tasks undertaken by nation states' law enforcement and security agencies. Today, the nature and scale of that threat have stimulated the creation of transnational criminal intelligence-sharing structures and processes.

We use this case to critically assesses information sharing between law enforcement agencies (LEAs). Our analysis is founded on narrative inquiry and experiential knowledge. It also draws upon empirical research into police intelligence practice conducted by the second author (2016 and 2017) and by the second author and others (Author 2 *et al*, 2017). Increasingly, it is understood that information management is a vital component of policing and security plans. Intelligence has become a basic police tool for crime-fighting and for the maintenance of security (den Boer, 2002 and Tilley, 2016). That has significant implications for law enforcement agencies, their stakeholders and those under agencies' protection. It is important in the context of the legality and effectiveness of state institutions' intelligence practices, citizens' freedoms and fundamental human rights because the former have the potential to threaten the latter to a greater extent than almost any other aspect of public policing.

Europol's crime analysis system (ECAS) may provide a useful template for the future development of international and transnational networked systems. Europol claims that such a system can allow LEAs to respond lawfully and effectively to the increasing dangerousness of the social world, to maintain their legitimacy and to demonstrate their commitment to the protection of citizens' rights and fundamental freedoms (Europol, 2018). Yet, no matter how well they have been designed, these developments also signal the limits of structures and processes in this context. The paper argues that no intelligence system can function effectively without trust, which nurtures connections and nodes so that relationships between individuals and organisations are durable and productive.

Europol’s origins and structure

Representing one of the first attempts to create an international policing organisation capable of countering transnational offending, Europol was established by Article K1 of the Treaty of Maastricht (Treaty on European Union, signed 7 February 1992; entered into force 1 November 1993). In 1998, the Europol Convention was ratified and it entered into force in October of the same year. The institution officially began operations on 1 July 1999. Today, it represents the EU’s most comprehensive and formal node of crime intelligence practice in the fight against cross-border threats. Europol styles itself as a support centre for law enforcement operations, a hub for criminal information, and a centre for law enforcement expertise. About 20% of its staff are liaison officers seconded from Member States (MS) (Europol, 2018).

Europol's mission is to support and strengthen actions taken by EU MS’ law enforcement agencies. It supports MS’ mutual cooperation to prevent and combat serious crime affecting two or more of their number. It also sustains activities to combat terrorism and other forms of crime affecting MS’ interests (as set out in EU policy). With more than 1,000 staff, Europol provides multilingual and multinational crime intelligence expertise from its headquarters in The Hague to LEAs across the EU and in its partner countries. It supports more than 40,000 complex transnational organised crime and terrorism cases every year (Europol, 2018).

Europol’s powers and competences

Europol does not have autonomous investigative capabilities and never directs operational activities (which always are solely the responsibility of EU MS). Europol’s representatives do not have the normative rights of crime intelligence services. For example; the lawful power to intercept telecommunications, covertly observe persons or places, or to manage informers are the preserve of the competent national authorities. However, Europol can make tangible contributions to law enforcement cooperation within the EU by: proposing common strategic frameworks (for example, the European Agenda on Security 2015-20); improving information exchange (for example, by managing databases such as the Schengen Information System); promoting operational cooperation; cooperating on specific operations; and by funding training, research and innovation in MS (Europol, 2018).

Europol's crime intelligence competences have their basis in EU treaties and in international law. The institution’s forms and methods of analysis, interpretation and exchange of crime information are consistent with the already well-established practices of international policing. Europol undertakes intelligence-gathering activities but the application of coercive measures is the exclusive responsibility of the competent national authorities. Operational actions invariably are carried out according to the statutes and regulations, and - not least – the wishes, of the MS concerned (Europol, 2018).

Europol’s criminal intelligence process

At the strategic level, Europol adds value to information provided by MS, to produce strategic diagnoses of risks associated with transnational threats via its: Serious and Organised Crime Threat Assessment (SOCTA); Internet Organised Crime Threat Assessment (IOCTA); and EU Terrorism and Situation and Trend Report (TE-SAT). These strategic reports have been described as Europol’s ‘most important intelligence products’ (Ballaschk, 2015 p.37). At the tactical level, crime intelligence work carried out by Europol is supportive of and complementary to the intelligence functions of the MS; serving to increase the efficiency and functionality of the latter (Europol, 2018). Thus, at the operational level where the intensity, extent or nature of a threat challenges the ability of an MS to counteract it, Europol can lend its support; helping to collect, store, analyse and disseminate information between nations (Author 1, 2013).

Europol’s primary responsibilities are to notify EU MS, via Europol National Units (ENUs), of information and connections between criminal offences concerning them and to coordinate, organise and implement investigative and operational actions to support and strengthen actions by the competent authorities of the MS, where appropriate. In liaison with Eurojust; Europol proposes and participates in joint investigation teams; providing information and analytical support to MS in connection with major international events; preparing threat assessments, strategic and operational analyses and general situation reports; and developing, sharing and promoting specialist knowledge of crime prevention methods, investigative procedures and technical and forensic methods. It provides advice to EU MS; operational, technical and financial support; and specialised training or assistance to MS in organising training in coordination with the European Union Agency for Law Enforcement Training (CEPOL). Moreover, it provides information and support to: EU crisis management structures and missions; centres of expertise for combating certain types of crime falling within Europol's objectives, which are facilitated, promoted or committed using the Internet; strategic analyses and threat assessments to assist in laying down strategic and operational priorities of the EU; and assists the efficient and effective use of EU resources for operational activities in MS.

Europol’s Crime Analysis System (ECAS)

Europol’s task in this context is the legal and effective systemization of its data collection, analysis and evaluation practices. The intended outputs of those endeavours are intelligence products that help MS in their prevention, diagnosis and detection of transnational threats. The system draws on information from open sources and a number of discrete databases. It is represented diagrammatically at Figure 1.

Figure 1 – Europol’s Crime Analysis System here

The ECAS process

As the figure shows, the process is executed according to the following phases: the identification of an organised crime group or terrorist organization through operational analysis; the location of the organised crime group or terrorist organization through the exchange of information between MS and Europol; neutralization of the organised crime group or terrorist organization (terrorists) by the MS (e.g. through arrests, detentions, disruption activity), with Europol’s analytical and other support; and the provision of feedback to MS via Europol’s systems and databases.

In Europol’s combating of organised crime and terrorist threats at the strategic level, the following phases can be distinguished: first, the identification of criminal or terrorist phenomena as a result of its strategic analyses; second, location of the criminal or terrorist phenomena through the exchange of information between MS and Europol; third, neutralization of the criminal or terrorist phenomena through joint action by MS, international organizations and Europol (for example, through the development of programmes of international activities) (Author 1, 2013).

The concepts of identifying, localizing and neutralizing transnational threats require explanation. These terms refer to the function of forensic science, which distinguishes the following functions: reconnoitring; detecting; preventing and proofing (Hanausek, 2005). Reconnoitring develops methods and measures calculated to obtain the greatest possible amount of information about the activities and plans of criminals/terrorists. It aims to bind the criminal/ terrorist acts with mechanisms that may bring about change. Detecting, aims to cement the operational knowledge obtained in the process of reconnoitring. Preventing, is taking action to neutralize the negative pressures and prevent abstract threats predicated on the basis of experience and research or analysis.

Activities undertaken within the framework of proofing, include the forensic assessment of the probative value of evidence (Gruza *et al*, 2008). Thus, in combating transnational crime, reconnoitring and detecting routinely are associated with the identification of threat, while neutralization more usually features acts that amount to preventing or proofing. In both cases, ECAS seems – in principle - to provide an efficient and effective vehicle for the lawful and proportionate sharing of data (Author 1, 2017). In practice the process of identification, localization and neutralization of transnational crime may include the following discrete activities: -

1) Identification of problem by Europol;
2) exchange of information within Europol;
3) identification of criminal relationships with other countries;
4) initiation of analysis in the form of an AWF;
5) identification of further criminal relations with other countries;
6) exchange of intelligence between interested MS;
7) cooperation between MS' investigators through operational meetings;
8) preparation of international operations (supported by Operational Center 24/7);
9) direct analytical support (provision of mobile offices and experts);
10) information exchange with Eurojust.

Significant Europol databases

Three databases probably have the greatest significance to Europol's work: Europol's Information System (IS); the European Bomb Data System (EBDS); and the Europol Analysis System (EAS) (Author 1, 2017). IS primarily is used to support investigations. The system collates and evaluates crime information collected by MS and submitted to Europol. It also is the repository for relevant data collected by Europol staff. Its functions include the abilities to search, visualize and link information. Linking of data allows for cross-checking so that information about the same objects (persons, means of transport or communication, addresses) can be grouped and classified. Common elements in putatively discrete cases are determined and information exchanged via Europol in a standardised manner.

EBDS is a database of seized explosive devices. Data are collected in text and multimedia form (e.g. images and diagrams of electronic devices). The database provides European LEAs with information about explosive devices, pyrotechnic materials or their components. The EAS is an operationally-focused information system that hosts data contributed by Europol's stakeholders. The data collected is analysed using a wide range of tools. EAS is based on AWFs. These gather together operational and personal data, providing material for comprehensive operational analyses of criminal activities. AWF can be considered to have two dimensions; a technical tool that organises the analytical work and also a tactical entity that organises and focuses analytical and information-sharing activities.

Examples of those work files are 'Dolphin' and 'Islamic Terrorism' (Europol.2018). Both explore the threat from terrorism at the tactical level. In both cases, Europol analyses specific features of terrorism, terrorist organizations and terrorists operating in MS. Intelligence can provide the impetus for the security services of the MS to initiate investigations or to implement police operations. Where MS choose to commission Europol, the latter provides them with operational expertise in the form of crime analysis and other specialist services.

Asset recovery and financial investigation

Europol has stated that an important element in combating criminal networks is understanding the financial aspect of their activities (Europol, 2018). Organised crime is big business, costing EU citizens tens of billions of Euros annually. The loss in tax revenues also has direct impacts on public finances and on public confidence in the ability of the EU and its MS to combat it (Bakowski, 2015). Europol's published policies and plans aim to support EU MS actions against organised crime. Particularly, MS' efforts to identify and localise the assets of those involved with organised crime or terrorist activity (Europol, 2018).

The system of cooperation between national asset recovery offices is complemented by the work of the Camden Assets Recovery Interagency Network (CARIN). Supported by Europol (which acts as the secretariat for CARIN), it provides a framework for the exchange of information and experiences regarding the identification, freezing, seizure, and confiscation of funds related to criminal or terrorist activity. CARIN creates a system of national police contact points that are utilised to identify property and other assets located abroad (Author 1, 2010).

In the context of counter-terrorism, Europol's financial intelligence capability is supported by the agreement concluded between the USA and the EU (on 28 June 2010) on the processing and transfer of financial data under the provisions of the Terrorist Finance Tracking Programme (TFTP). This agreement allows for the lawful exchange of financial intelligence between the USA and the EU via Europol. In order to meet its obligations under the agreement, Europol maintains a specialized team of experienced IT experts and financial analysts (Europol, 2018).

Assessing the success of ECAS

The introduction of ECAS promised to give a new impetus to Europol's efforts to combat transnational crime (Europol, 2018). In principle, underpinned by treaty and an institutional respect for national regulations and legal norms, ECAS can promote effectiveness, transparency and intelligence practice that respects human rights and citizens' freedoms. However, it is axiomatic that any intelligence system is only as good as its inputs, and researchers have found evidence that the system is being undermined by MS' reluctance to share information - particularly sensitive information - with each other and with Europol (den Boer, 2015; Bures, 2008). The second author of this paper consistently has found information-sharing between police organisations and their partners to be sub-optimal (Author 2, 2013, 2016, and 2017). Specifically, in the context of this analysis, Author 2 found that ENUs routinely sought from/shared information with their own liaison officers at Europol headquarters; few of those communications were recorded in the institution’s memory (Author 2, 2016).

Shortcomings in the information management process

Arguably, one of the most important measure of the effectiveness of Europol's crime intelligence model is the number and quality of information reports it attracts. Europol cannot carry out its operational work effectively without comprehensive and timely reports from MS. As was noted earlier, Europol's crime intelligence competences have their basis in EU treaties and in international law. Largely, those treaties and laws are permissive. That is, actions and behaviours are permitted, rather than prohibited, by those treaties or laws. In the context of this analysis, it follows that those treaties and laws allow for the lawful exchange of information between MS and between MS and the EU and its agencies but they cannot, and do not, compel or otherwise oblige MS to share. Too often in practice, information-sharing is sub-optimal (den Boer, 2015, UK HLEUC, 2008). That makes it nigh on impossible: to determine accurately the specific effects of the measures taken by Europol; to assess the real significance of Europol’s interventions; or to properly understand the extent to which the institution is able to meet the expectations of its stakeholders.

This phenomenon is not unique to Europol; in the law enforcement milieu, it is both institutionally and culturally consistent (Berry *et al,* 1996). Author 1 (2013) has argued that too often in the European setting, attention to the lack of meaningful outcomes from an initiative or operation is deflected by institutionally-driven celebration of the process or the commitment to multi-national cooperation that the process engendered.

James Sheptycki’s (2004) research provided significant evidence of policing organizations’ reluctance to share information; considerable organizational and technical obstacles to sharing information routinely were erected by the institutional actors he observed. Eric Lichtblau (cited in Brodeur and Dupont, 2008 p.25) highlighted that the withholding of information by police organisations was a process that ‘feeds on itself’. Agencies fail to share information with partners so as to protect their own knowledge interests; their claims that they are ignorant of partners’ needs simply is the means by which they justify inaction (Ibid.). Though, political imperatives cannot be ignored, it is argued that the focus routinely should be on outputs and not on process (Author 1, 2013).

A question of trust

Scholars have argued that trust; sometimes, more accurately, distrust is at the heart of the information-sharing dynamic (see for example Brodeur and Dupont, 2008). There is evidence of dysfunction in Europol’s relationships with MS; practitioners sometimes seem reluctant to share information - particularly when that sharing goes beyond their own operating environment (Author 1, 2017 and 2018; Author 2, 2017). Nick Tilley (2005 cited in Brodeur and Dupont, 2008 p.9) argued that trust provides a safeguard against the ‘malfeasance, mistakes and failures’ of members but too often that is in short supply. Arguably, lack of trust in Europol limits the institution’s ability to collect the information it feels it needs (Occhipinti, 2015; den Boer, 2015; HLEUC, 2008). While it is accepted that intelligence pictures invariably are partial and confused, one cannot reasonably expect Europol’s analysts to deliver comprehensive analyses in these circumstances. Without that ‘missing’ information, the value of their intelligence products is bound to be limited. Moreover, knowledge that might be corroborated by one or more of those direct communications may go uncorroborated and information held in ECAS that could be validated objectively may remain unconfirmed and its value undetermined.

It is recognised that trust encourages the development of strong and enduring collaborations (Brodeur and Dupont, 2008). In their study of the UK intelligence milieu, Author 2 *et al* (2017) found little evidence of trust, or indeed strong and enduring collaboration between institutions. For example, even though research respondents said that they recognised the importance of engaging with partners and communities and of building trust with others, they acknowledged that officers needed more encouragement to build relationships and that more should be done to develop external relationships. One respondent said that intelligence ‘processes and protocols inhibited, rather than encouraged the free flow of information' (Author 2 *et al*, 2017 p.86). Conversely, researchers have found that the value of trust in this context seems to be better appreciated by individuals who have proved adept at building their own, often cross-cultural, communication networks and partnerships. For experienced practitioners (or at least those well-connected), national boundaries are no barrier to such exchanges (Author 1, 2013; den Boer, 2015).

Enshrined in The Hague Programme (which introduced the concept of direct access to information), the principle of availability also may limit the information shared by MS with Europol. The principle is meant to support the rapid and timely transfer of information between MS. It allows LEAs lawfully to exchange ballistic data, fingerprint traces, DNA, vehicle registration information, telephone numbers, and the minimum required to identify an individual. This establishes the conditions necessary for the rapid and seamless exchange of information on those subjects between the competent authorities of the MS. In practice, it also gives MS the opportunity to bypass Europol. Therefore, the principle actually may limit Europol's effectiveness because the information cannot be used by anyone other than those involved in the transaction.

Arguably, in both cases (peer-to-peer sharing and in instances where the principle of availability is cited), knowledge is shared only with selected insiders and does not land in those central nexus points where it can be analysed and evaluated more formally for the benefit of the institution and its partners and it can be incorporated into institutional memory. Therefore, behaviour that seems to demonstrate increasing interactivity may perhaps be better understood as evidence of isolationism (Author 2 *et al,* 2017). That should be of significant concern to stakeholders - because Europol's efforts in this context may be rendered ineffective – and to citizens because information-sharing may be less transparent and therefore less accountable than it should be.

Mapping cooperation in action

The following scenario outlines how the ECAS system can work in principle. Though it should be noted that trust, of the kind assessed above, usually is more easily gained by actors in tactical or *ad hoc* situations like the one we will describe. In such situations, the aims of the exchanges of information and services can be agreed face-to-face; the products of those exchanges are more obvious and more tangible (in terms of arrests, seizures of contraband and criminal profits). Arguably, a commitment to reciprocity is a key factor in strong and enduring formal information-sharing arrangements (Author 2 et al, 2017). We argue that is more difficult to achieve at the institutional level. Putative partners may not demonstrably share the same aims, the benefits to each of the partners of any relationship established, may be less obvious or less quantifiable immediately, and – simply - it is harder to build trust via email or other online communication than it is through human interaction (Furumo and Pearson, 2006; Zheng et al, 2002).

In this fictional case, the Spanish police receive information about the production of amphetamine in Poland. Information is passed to the Spanish liaison officer at Europol (through the Spanish ENU). She makes direct contact with her Polish counterpart who sends the information to the appropriate police department in Poland. Through simple operational actions at the drug factory (such as interviews and observations), the Polish police identify vehicles registered in Britain and in France. They update the Polish liaison officer who then discusses these initial findings with her Spanish, British and French counterparts.

The British and French liaison officers report the movements of the vehicles to their own national services. The British officer finds that the British vehicles are of interest to its National Crime Agency (NCA). Intelligence suggests they are associated with an organized crime group specializing in drug smuggling. The liaison officer group discuss these findings then relay them to their own ENU with requests for further instructions. In the meantime, the Polish police make further investigations into the property, vehicles and persons. The material collected allows for the initiation of an operational control (information obtained as a result of it may be transferred to an AWF). Further working meetings are held in The Hague where information is exchanged, findings discussed and proposals for further action made.

Europol liaison officers and analysts gather, analyse and disseminate information from the participating MS (in an AWF). Its analysts identify criminal relationships in other countries (revealed by personal contacts, telephone calls, bank transfers and so on). Europol hosts working meetings but acceptance or rejection of the analysts' advice is the prerogative of the competent authorities of the MS. All investigative activities are conducted under the exclusive competence of the police and other LEAs of the MS concerned. Europol's final contribution to these activities is the coordination of the tactical phase of the investigation through its 24/7 operational centre, supporting the operation through mobile offices, expert on-site consultations and information exchange (Europol, 2018).

In this scenario, we discussed the competence and the capability of Europol and of the LEAs in each of its MS. As we have shown, the legality of these activities is not in question but it is not law or treaties that ensure that these actions are carried through and investigations brought to successful conclusions. Those successes depend on structure - the framework that supports the investigation (the ECAS), agency – the motivation and capability of the people tasked with those undertakings – and critically, the extent to which individuals can see that the demands made upon them are balanced by the potential rewards. Researchers have found that trust seems to be much better appreciated by the kind of task-focused individuals we have described in our scenario, who have proved adept at building their own, often cross-cultural, communication networks and partnerships. For experienced practitioners (or at least the well-connected), national boundaries seem to be no barrier to such partnerships (Author 1, 2013; den Boer, 2015). Conversely, *a priori,* it is much more difficult for LEAs to achieve this level of trust at the institutional level. Certainly, few can bring forward evidence of their success in that regard; even if some have claimed it.

Conclusion

It is only natural that the perception of the social world as increasingly dangerous should stimulate the development of policing systems that attempt to harness information to deliver intelligence-led responses to crime. ECAS represents a lawful and ethical system for sharing criminal intelligence across borders. One that in principle, can act as a template for intelligence practice elsewhere. However, this study suggests that for all its merits, the system is neither operating as efficiently nor as effectively as it might.

There are some grounds for believing that ECAS can deliver at the tactical or operational level where the necessary legal and organisational frameworks are in place and, normatively, a focus on the task and its shared benefits drives action. However, at the institutional level, shortcomings in the information-sharing process - where the same frameworks are in place but the focus on task and shared benefits seems lacking - undermine Europol's efforts to manage risk, to identify, localise and neutralize transnational threats or to assign the right tools to transnational policing problems. That should come as no surprise. Few law enforcement agencies can claim meaningful success in that regard

There seems a need for greater reflection by policymakers and practitioners within Europol, MS and the wider law enforcement community on the processes of information-sharing. We wonder, even as the social world embraces virtual and asynchronous communication, whether institutions can find clues to strategic success in the tactics they employ at the operational level. Notwithstanding that, the search for answers may need to go far beyond classical ideas of policing, venturing into the fields of political science, psychology, and sociology where researchers have embraced new ways of thinking about networks and intra and inter-agency information transfer. We argue that finding those answers not only is in the interests of Europol, its stakeholders and its law enforcement partners in the name of efficiency and good governance but also in the cause of transparency and accountability to the communities it serves.

References (those associated with the authors have been omitted)

Bakowski, P. (2015). *Organised Crime in the European Union*. Brussels: European Parliamentary Research Service.

Ballaschk, J. (2015). In the Unseen Realm: Transnational Intelligence Sharing in the European Union - Challenges to Fundamental Rights and Democratic Legitimacy51 *Stan. J. Int'l L*.19.

Berry, G. (1995). *Practical Police Management*. London: New Police Bookshop.

Brodeur, J-P. and Dupont, B. (2008). The role of knowledge and networks in policing in T. Williamson (Ed.). *The Handbook of Knowledge-Based Policing: Current Conceptions and Future Directions*. London: John Wiley & Sons, pp.9-33.

Bures, O. (2008). Europol's Fledgling Counterterrorism Role. *Terrorism and Political Violence.* Vol.20, Iss.4.

den Boer, M. (2002). Intelligence Exchange and the Control of Organised Crime: in Europeanisation via Centralisation to Dehydration, in J. Apap and M. Anderson (Eds.) *Police and Justice Co-operation and the New European Borders.* Amsterdam: Kluwer Law International.

den Boer, M. (2015). Counter-Terrorism, Security and Intelligence in the EU: Governance Challenges for Collection, Exchange and Analysis, *Intelligence and National Security*, 30/2-3, pp.402-19.

EU Council (2005). *The Hague Programme: strengthening freedom, security and justice in the European Union*, OJ of EU C 53/1 of 3 March 2005.

Europol (2018). *About Europol*. Europol's structure and purpose - Europol website at https://www.europol.europa.eu/content/page/about-us

Furumo, K and Pearson, JM (2006, January). An empirical investigation of how trust, cohesion, and performance vary in virtual and face-to-face teams. In *System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference* on (Vol. 1, pp.26c-26c). IEEE.

Gruza, E.; Goc, M.; and Moszczyński, J. (2008). *Kryminalistyka - czyli rzecz o metodach śledczych*, Warsaw: Wydawnictwa Akademickie i Profesjonalne, p.22-30.

Hanausek, T. (2005). *Kryminalistyka*, zarys wykładu, Krakow: Zakamycze, pp.38-41.

HLEUC (2008). House of Lords European Union Committee, 29th Report of Session 2007–08, *EUROPOL: coordinating the fight against serious and organised crime*. London: HMSO.

Occhipinti, J. (2015). Still Moving toward a European FBI? Re-examining the Politics of EU Police Cooperation. *Intelligence and National Security* [2015], 30, pp.2-3.

Tilly, C. (2005). *Trust and Rule.* Cambridge: Cambridge University Press.

Sheptycki, J. (2007). High Policing in the Security Control Society. *Policing* 1(1), pp.70–79. doi:10.1093/police/pam005.

Tilley, N. (2016). Intelligence-led policing and disruption of organized crime: motifs, methods, and morals in T. Delpeuch and J.E. Ross (Eds.) *Comparing the Democratic Governance of Police Intelligence: New Models of Participation and Expertise in the United States and Europe*. New York: Edward Elgar.

Zheng, J; Veinott, E; Bos, N; Olson, JS; and Olson GM (2002). Trust without touch: jumpstarting long-distance trust with initial social activities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '02). ACM, New York, NY, USA, 141-146. DOI=http://dx.doi.org/10.1145/503376.503402

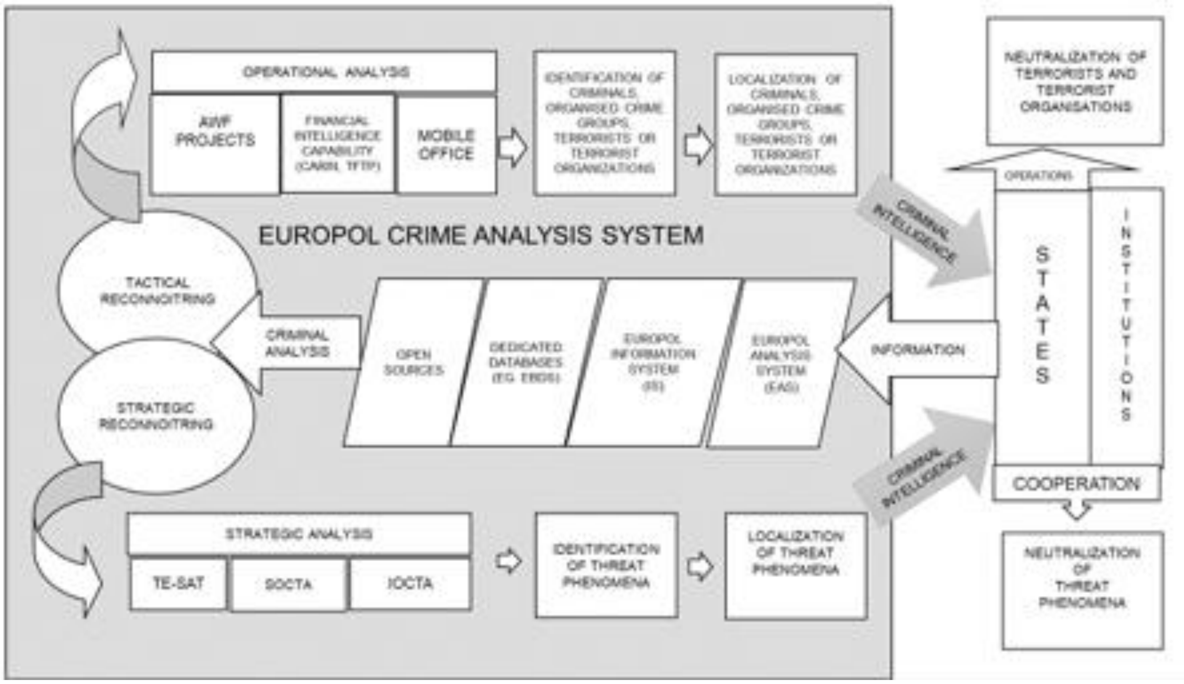
OPERATIONAL ANALYSIS
AWF PROJECTS
FINANCIAL INTELLIGENCE CAPABILITY (CARIN, TFTP)
MOBILE OFFICE
IDENTIFICATION OF CRIMINALS, ORGANISED CRIME GROUPS, TERRORISTS OR TERRORIST ORGANIZATIONS
LOCALIZATION OF CRIMINALS, ORGANISED CRIME GROUPS, TERRORISTS OR TERRORIST ORGANIZATIONS
NEUTRALIZATION OF TERRORISTS AND TERRORIST ORGANISATIONS
OPERATIONS
EUROPOL CRIME ANALYSIS SYSTEM
CRIMINAL INTELLIGENCE
TACTICAL RECONNOITRING
CRIMINAL ANALYSIS
OPEN SOURCES
DEDICATED DATABASES (EG. EBDS)
EUROPOL INFORMATION SYSTEM (IS)
EUROPOL ANALYSIS SYSTEM (EAS)
INFORMATION
STATES
INSTITUTIONS
STRATEGIC RECONNOITRING
CRIMINAL INTELLIGENCE
COOPERATION
STRATEGIC ANALYSIS
TE-SAT
SOCTA
IOCTA
IDENTIFICATION OF THREAT PHENOMENA
LOCALIZATION OF THREAT PHENOMENA
NEUTRALIZATION OF THREAT PHENOMENA

Figure 1