UACES 46th Annual Conference

London, 5-7 September 2016

www.uaces.org

Artur Gruszczak
Associate Professor of International Relations
Jagiellonian University
Krakow, Poland
artur.gruszczak@uj.edu.pl

EU criminal intelligence cooperation – challenges of oversight and accountability

Paper to the UACES 46th Annual Conference, London, 5-7 September 2016

Introduction

The European Union for more than a decade has developed forms and mechanisms of criminal intelligence. The European Criminal Intelligence Model, intelligence tradecraft practiced by Europol and networked arrangements of criminal information exchange and intelligence sharing are examples of the widening scope of cooperation between EU Member States and relevant agencies and bodies. As a result of this cooperation, the bulk of information discreetly provided by member states is held and processed at EU level. EU agencies transfer sensitive data and handle a wide variety of intelligence deliverables. The contentious issue of oversight of intelligence activities and accountability of services and bodies involved in intelligence sharing has also been identified with regard to criminal intelligence cooperation in the EU.

The issue of democratic oversight of intelligence services raises many controversies and poses some challenging questions about appropriate normative frameworks, procedures and instruments. It goes without saying that intelligence services and international forms of their co-operation are cloaked, at least to a

considerable extent, in a shroud of secrecy. In such conditions, any form of monitoring, control, supervision or, finally, oversight is confronted with considerable obstacles and meets certain difficulties (Gill &Phythian, 2012, pp. 170-2). The intelligence sector quite often defends itself against close monitoring and careful observation by the media and NGOs sensitive to issues of privacy, transparency and accountability. It seeks to be exempted from thorough review for the sake of its robustness, effectiveness and reliability. It is motivated by its unique capacities and exclusive entitlement to carry out secret activities concerning vital security issues and protecting public order and national interests.However, this 'exclusiveness' of the intelligence sector may generate serious risks and, sometimes, direct threats to the legitimate authorities, the legal order in the state and, last but not least, international relations. Intelligence, because of its contested tradecraft, secrecy and exclusiveness, as well as its tendency to engage in activities detrimental to privacy and individual freedoms, often poses serious moral and ethical dilemmas (Herman, 2004; Erskine, 2004; Sepper, 2010; Gill & Phythian, 2012).

An analysis of the oversight and accountability of EU intelligence cooperation is a highly demanding issue in terms of methodology. The generic model of intelligence oversight and democratic accountability applied to individual states and their political regimes does not necessarily fit the structure and logic of EU intelligence co-operation. One should also bear in mind that EU intelligence cooperation has steadily evolved from dispersed and varied forms of co-operation to a genuine organizational form of intelligence sharing. Therefore, this paper elaborates on the concept of tri-dimensional accountability. It underscores the peculiar aspects of intelligence co-operation in the EU by analysing oversight and control functions performed by EU institutions and bodies in two dimensions: horizontal and vertical. It also frames the complexity of EU intelligence control mechanisms in the context of tensions between national scrutiny and supranational oversight. The paper builds on the observation that institutional oversight includes a set of measures, procedures and mechanisms generated at the intersection of separate ambits of intelligence management and tradecraft practiced in the EU by its agencies and Member States. It advances the thesis that oversight and accountability of EU criminal intelligence cooperation are subject to disaggregated

policy arrangements established at different levels of co-ordination of knowledge management practices in the realm of EU internal security cooperation.

Oversight and accountability in intelligence cooperation

Oversight refers to a set of activities that are used to carry out a thorough, careful and structured scrutiny of an entity (an individual, an organisation or a network), aiming to evaluate the compliance with the binding rules, principles or criteria, such as effectiveness, validity or transparency (Baker, 2008, pp. 201-2). It includes formal and informal, general and detailed measures and procedures covering all aspects of the entity's behaviour or performance or focusing on specific areas (Wills et al, 2011, p. 41).It also entails the informal and formal scrutiny conducted by the legislature with regard to the observance of constitutional principles, legal norms and regulations. Moreover, it is pertinent to the supervision of intelligence activities by members of the executive branch with regard to the quality and effectiveness of intelligence bodies, especially secret services, in the fields of national security, public order and the individual safety of the citizens.

Oversight is closely tied to the notion of accountability. In the institutional perspective, accountability is a set of organisational arrangements created for the checking and overseeing of agents in terms of established patterns of their behaviour. In the functionalist perspective, it is a precondition of the legitimacy, transparency and efficiency of actors and modes of their performance in a pre-defined systemic setting promoting mutually beneficial co-operation (Grant and Keohane, 2005, pp. 31-2; Keohane, 2006, p. 76; Bovens, 2010, pp. 954-5). In the normative perspective, it is associated with mechanisms and procedures for enforcing rules and executing sanctions in event of a breach of the normative order. Control and punishment underpin the regulatory function of accountability as a relationship, ensuring the rule of law and preventing abuse of power in a complex governance system (Benz, Harlow & Papadopoulos, 2007, p. 443; Trechsel, 2010, pp. 1052-3).

At the theoretical level, the question of accountability and oversight in democratic regimes has been extensively discussed by scholars investigating social and political change. Guillermo O'Donnell introduced the concept of two

dimensions of accountability: vertical and horizontal (O'Donnell,1994, p. 64). The former concerns the sources of legitimate authority and the relationship between actors participating in power distribution (i.e. from citizens to elected leaders); the latter refers to autonomous agencies capable of calling into question and eventually punishing the misuse of prerogatives or the abuse of power by a public actor (Waldrauch, 1998, pp. 1-2). Robert Pastor (1999, p. 124) added the third dimension of accountability: international observation and supervision 'enhancing vertical accountability by making sure elections are successful and strengthening the horizontal axis by calling encroaching institutions to account for their actions.'

Marina Caparini adopted the concept of tri-dimensional accountability in her analysis of intelligence services. Starting with the vertical dimension, she underscored the importance of the executive as the branch state power responsible for tasking and directing intelligence services. Representatives of the executive can set policy guidelines, issue administrative acts or directly instruct the head and senior management of intelligence agencies. They can demand access to relevant information held by the services for the sake of national security and vital national interests. Top-down hierarchical control and supervision are also enforced within the institutional framework of intelligence services by the head of the intelligence sector or directors of individual agencies. Bottom-up accountability is specific in intelligence services; it occurs in exceptional cases, taking the form of 'whistleblowing' as an internal accountability mechanism used to draw public attention, or even the state authorities' concern, to mismanagement, malfunctioning or direct threats to national security or the public interest. More often and 'normal' is self-accountability and exact compliance with professional norms and administrative directives (Caparini, 2007, pp. 10-11). The vertical dimension also involves non-state actors: citizens, non-governmental organisations, advocacy groups and media. None of them is formally entitled to supervise intelligence authorities. They conduct 'undersight' ('sousveillance'), tracking official surveillance practices and expressing concerns (van Buuren, 2013, p. 250). They ensure the constant monitoring and close watch on the intelligence sector and alert the public when fundamental interests or civil liberties are in jeopardy. The media as the 'fifth power' occupy a prominent role due to their much wider access to information and capacity to contact the representatives of state

authorities, including the intelligence sector. They can also articulate public opinion, voice citizens' concerns and provide feedback to state security institutions and authorities (Caparini, 2007, pp. 12-13).

The horizontal dimension is based on inter-institutional connections and is determined by the distribution of competences and duties among parallel power branches. The typical separation of powers and the checks-and-balances system are the foundations of democratic government, enabling inter-related safeguards for constitutional principles and national security. The steering and management functions performed by the executive are subject to internal control mechanisms and procedures which are sometimes subject to politicisation and partisanship. Consequently, the legislature assumes the role of the 'guardian' of democratic control and oversight. Parliamentary scrutiny is often regarded as the most effective means of supervision over intelligence institutions and the mechanism of correction or reform of the intelligence apparatus. The parliament establishes the legal framework for the intelligence sector, sets the competences, rights and duties of intelligence services, exercises general oversight and decides on financial resources. Parliamentary committees can request information from representatives of intelligence services and organise hearings (Caparini, 2007, p. 13). The judiciary exerecises independent prerrogatives to monitor how the other branches act within the legal framework and particularly to prevent the executive from exercising power arbitrarily (Leigh, 2011, pp. 75-6). Judicial review gives the courts the power to interpret laws and veto those acts which undermine constitutional and legal order (Caparini, 2007, p. 15). Independent oversight entities are an important addition to the vertical configuration of accountability. The offices of ombudsman, data protection supervisor or national auditor can investigate procedural irregularities and administrative failings.

The third dimension of accountability addresses the question of what impact external (international) actors can have on the functioning of national intelligence agencies. Caparini argues that the role of the international community is increasingly significant in spite of the sovereignty principle and protective measures adopted by national governments. Intergovernmental organizations, such as the Council of Europe or NATO, international courts, like the European Court of Human Rights, and even international NGOs can exert a direct influence on

national intelligence services. They can reveal secret information and launch international investigations (as was the case of the so-called CIA rendition flights). They can even set some standards with regard to oversight and accountability (Caparini, 2007, pp. 16-17).

The tri-dimensional accountability model is appropriate to study EU criminal intelligence cooperation. Although the powers conferred on EU institutions and agencies involved in information exchange and intelligence sharing are considerably limited (see Bono, 2006, p. 442), the density of sense-making and intelligence networks as well as the tendency to adopt a comprehensive approach to the management and political supervision of intelligence cooperation makes it necessary to work out and implement multiple forms and mechanisms of oversight and control at the EU level. However, the sensitivity and often secrecy surrounding data, information and analytical material exchange between national services and EU agencies predetermines the competences and real meaning of EU oversight and control. The principle of national originator and respect for 'national ownership' of information and intelligence transmitted to the relevant EU agencies and units has a tremendous impact on oversight and control in practical terms. This is why the vertical dimension is so explicitly highlighted by inter-governmental arrangements functioning at the level of EU intelligence co-operation. For the governments of member states, their presence in the Council of the EU and its working bodies is not always sufficient. They seek to tighten their grip on information management in the security field through the establishment of joint supervisory authorities. Equally, national supervision may be strengthened by national parliamentary oversight insofar as the required EU legislation is adopted.

In the vertical setting, the activities undertaken by social actors, advocacy groups and media are important nonetheless, given that they indicate the areas exempted from 'normal' monitoring and control and thereby posing certain risks for fundamental rights, civil liberties and democratic politics. This special 'sousveillance' embodies the collective sensitivity to the monstruous secret intelligence apparatus wanting to conquer the public space in order to enslave 'the European citizen'. So, sousveillance 'focuses on enhancing the ability of people to access and collect data about their surveillance and to neutralize surveillance.' (Mann, Nolan and Wellman, 2003, p. 333). Several NGOs, independent advocacy

groups and media outlets, such as Statewatch, the Transnational Institute, EU Observer.com, Telepolis or Euractiv.com have been systematically observing developments in EU intelligence co-operation.

Monitoring and oversight activities have also been performed by actors belonging to the third dimension. However, they have not been intense and far-reaching because of the specific nature of the EU intelligence community, its trans-governmental dimension and multiple membership of the majority of EU Member States in international organisations performing oversight activities (such as the Council of Europe, the Venice Commission or the OSCE).

In most EU Member States international intelligence co-operation is a politically sensitive issue and 'an under-scrutinised area of services' work.' (Leigh, 2015, p. 1).This has to do with the fact, highlighted by Gill and Phythian (2012, p. 177), that security intelligence is 'low visibility work' requiring an extensive scope for discretion. The reasons are manifold: the sovereignty principle, the predominance of national oversight authorities, the soft competences of international scrutiny bodies, restricted access to information, deficit of trust. Therefore, the responsibility for control and oversight rests on national institutions according to binding legal regulations and in conformity with the powers conferred. When information, data or intelligence are transmitted up to the EU level, they are already checked for their availability to external actors. This question arises when a given piece of information, or a national intelligence input, is entrusted to supranational agencies and loaded into computer information systems connecting numerous national users in a central hub managed by EU institutions. In such conditions, the oversight entails the management of data stored in EU information systems; the supervision of authorities responsible for the proper handling of information received and delivery of intelligence products; the control of the correct application of EU norms regulating access to information, in particular that covered by a confidentiality clause; the checking of whether information and intelligence products are strictly related to the given categories permitted by the law.

EU intelligence-driven agencies and units do not possess autonomous operational capabilities and as such avoid controversial and risky activities which could bring about a general outrage, public protests or political skirmishes. Hence,

no dramatic actions and contentious operations, such as covert actions, eavesdropping or infiltration, have occurred. However, in multiple cases of controversies surrounding the management of information by EU agencies and bodies, the transfer of sensitive data to third countries and the control of the way information and intelligence is used by EU agencies and units have stimulated political discussion and proposals for enhancing oversight and scrutiny of the EU intelligence activities.

EU Criminal Intelligence – foundations and basic elements

For centuries, crime in its many embodiments has posed a huge and constant challenge for institutions and services in charge of maintaining public order and enforcing law. Acquiring, gathering, compiling, comparing, analyzing and sharing information and data on individuals or activities suspected of being, or known to be, criminal in nature was one of the most relevant activities in the realm of national and international security. Criminal intelligence was formed as an organized state response to proliferation of criminal threats and activities. According to a definition of the Global Justice Information Sharing Initiative, criminal intelligence is identified as 'Information compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity.' (US Department of Justice, 2003).

The development of police and criminal justice cooperation in the EU since the late 1990s, particularly following the establishment of the European Police Office (Europol) in 1999 and the European Judicial Cooperation Unit (Eurojust) in 2000 (fully fledged since 2002), gave EU member states solid bases for coordinated efforts and joint undertakings in the area of criminal prevention and investigation. The expansion and diffusion of criminality, especially serious forms of transnational organized crime, gave strong impetus for launching EU-wide operations engaging more and more national services and law-enforcement agencies. Terrorist threats, exploding on 11 September 2001, highlighted the critical importance of international cooperation for effective prevention and combating of terrorism and transnational crime.

Attempts at intensifying and enlarging the scope of judicial cooperation in criminal matters at EU level resulted in the adoption of several legal instruments and the pressure at Member States to implement the existing EU legal measures in this field. Efforts aimed to encourage a more intense and effective exchange of criminal information and intelligence did not yield the expected results, mostly due to the lack of unanimity and the deficit of trust among Member States (Bures, 2006, p. 62-63; Müller-Wille, 2006; Duke, 2006, p. 619-620).

After the 11 March 2004 terrorist attack in Madrid, EU institutions placed particular emphasis on the exchange of information and intelligence between law enforcement authorities of Member States and called for the improvement of mechanisms for cooperation and the promotion of effective systematic collaboration between police, security and intelligence services. The European Commission in its communication of June 2004 called for the setting up of a European Criminal Intelligence Model (European Commission, 2004, p. 8). This model would comprise a common methodology of a reliable threat assessment. It would eventually render intelligence-led law enforcement effective and allow for enhanced cooperation in the field of criminal justice. EU criminal intelligence would assist the competent national authorities in the performance of their strategic or operational tasks in order to prevent and combat terrorism and other forms of organised crime.

Member States also agreed to develop a criminal intelligence model. In the multi-annual programme of cooperation in justice and home affairs, adopted by the European Council in November 2004, they acknowledged that the national law enforcement services as well as units already established at the European level had an incomplete and rather poor awareness of serious and organised crime. Therefore, Member States should support EU agencies, such as Europol, in better access to criminal information and intelligence enabling the preparation of reliable threat assessment and situation reports and the setting up and implementing a methodology for intelligence-led law enforcement at EU level (European Council 2004, 9).

Terrorist attacks in London in July 2005 stimulated Member States to generate criminal intelligence capabilities at EU level. A British proposal submitted to Interior Ministers from EU Member States in September 2005 introduced the idea

of a European Criminal Intelligence Model (ECIM) based on the principles of intelligence-led policing. An ECIM consisted in a better knowledge of serious and organised crime through more effective collection, exchange, and analysis of information; increased effectiveness of Europol and other relevant EU bodies; a common methodology for tackling serious and organised crime in the EU (UK Presidency, 2005, p. 1).

The concept of EU criminal intelligence cooperation indeed took shape of an intelligence cycle which relied on inputs from Europol and Member States contributing either directly or through appropriate institutional or working schemes as provided in EU law. The elements of that cycle included strategic priorities on the basis of threat assessments delivered by Europol; intelligence requirements facilitated by Europol; storing and analysing intelligence in Europol; producing specialist threat assessments to improve knowledge in priority areas; identifying and targeting top criminals and networks by Member States; recycling through Europol intelligence generated by investigations underway (Council of the EU, 2006a, p. 3).

This cycle required operational excellence and demanded from national stakeholders (law enforcement agencies from Member States) full commitment to the principles of EU criminal intelligence cooperation and strong capacity to deliver requested information and data. It was a highly demanding task and not every Member State was ready, capable and willing to meet these requirements and expectations. As a result the European Criminal Intelligence Model did not achieve a full work capacity nor it was grounded on a comprehensive approach to intelligence tradecraft. One of the reasons behind the difficulties and delays in implementing the full criminal intelligence cycle was the lack of a single clear definition of intelligence.

While in December 2006 the Council finally adopted, on the initiative of Sweden, the framework decision on simplifying the exchange of information and intelligence between law enforcement authorities of EU Member States (Council of the EU, 2006b), it neither significantly improved the efficiency of information exchange system in the EU, nor did it contribute to the feasibility of the ECIM. A prospective solution to the challenge of granting mutual access to criminal records stored in the individual databases of the Member States, based on the principle of

availability, formulated in the Hague Programme and contained in the Swedish initiative, collapsed in the face of the inherent bureaucratic inflexibility within the decision-making process at the EU level.

The 2009 Stockholm Programme of the development of EU area of freedom, security and justice highlighted the necessity to establish a methodology based on common parameters in order to be able to analyse the threats at European level (European Council, 2010). It heralded a new strategic approach to internal security in the European Union. It was embodied in the EU Internal Security Strategy (EU ISS) adopted in early 2010 to further improve security in the EU, protect safety of citizens of the Union and tackle organised crime, terrorism and other threats. Building on some original premises of the ECIM, the new strategy focused on an intelligence-led, proactive approach to the challenge of terrorism, organised crime and both natural and man-made disasters. It highlighted prevention and anticipation as mechanisms aimed to detect future threats and prevent their happening. It called Member States to foster information exchange on a basis of mutual trust and share intelligence in time in compliance with the principle of information availability (Council of the EU, 2010a).

EU ISS offered a strategic framework and broad guidelines for a comprehensive approach to effective intelligence-led policing and enhanced criminal intelligence cooperation among EU Member States with a direct and active involvement of competent EU agencies and bodies (Bossong and Rhinard, 2013, p. 51-52; Horgby and Rhinard, 2013). It laid solid grounds for criminal intelligence conceived as a critical element of evidence-based cooperation in the area of criminal justice in the EU, supported by the best available assessments and risk analyses, and overwhelmingly accepted as a viable political option.

In October 2010, the Standing Committee on operational cooperation on internal security (COSI) agreed on the establishment of a EU policy cycle for organised and serious international crime on the basis of an intelligence-led policing approach. JHA Council adopted in November 2010 conclusions on the creation and implementation of an EU-wide policy cycle for organised and serious international crime. It was implemented in two stages: initial two-year policy cycle 2011-2013 and full-fledged four-year policy cycle 2013-2017 (Council of the EU, 2010b).

For the purposes of criminal intelligence, the policy cycle included:

- a complete and thorough picture of criminal threats reflected in Europol's serious and organised crime threat assessment (SOCTA);
- prioritisation of identified threats and adoption for each of the priorities of a Multi-Annual Strategic Plan (MASP) in order to work out a comprehensive response to the addressed threats involving preventive as well repressive measures;
- implementation of annual Operational Action Plans (OAP) built upon the COSPOL framework as the multilateral cooperation platform to address the prioritised threats;
- a thorough evaluation of outputs and outcomes of the cycle contributing to the formulation of intelligence requirements for the next policy cycle.

Belgian Presidency asserted in July 2010 that its proposal is nothing but 'a generic European Criminal Intelligence Model that describes a multi-annual policy cycle and defines the roles, processes and products needed for the implementation thereof.' (Council of the EU, 2010c, p. 1). The policy cycle sought to fill the gaps in the hitherto implementation of the ECIM and aimed to translate current strategies and political priorities into operational plans and appropriate activities. Although cyclical in its name, it was rather conceived as a temporally determined sequence of strategic assessments, political decisions and operational plans intended to bring about a better systemic response to the current and emerging threats (Council of the EU, 2010d).

Serious and organised crime threat assessment (EU SOCTA) was envisaged as a core element of full-fledged policy cycle. In June 2012 COSI approved the methodology used to produce SOCTA for the purposes of the policy cycle 2013-2017. SOCTA was defined as a present- and future-oriented threat assessment based on the analysis of the threatening features and aspects of serious and organised crime groups, areas of their activity and regional dimensions of those activities. It was relying on information and data provided by national law enforcement agencies as a response to intelligence requirements (questionnaires), delivered by third countries or organisations and extracted from open sources. The final result was an analytical ('intelligence') product comprising a list of recommended priorities supporting decision-making and the preparation of multi-

annual strategic plans on organised crime groups and serious crime areas (Council of the EU, 2012).

The policy cycle re-organised the institutional framework for EU criminal intelligence, referring directly to post-Lisbon EU architecture in the area of freedom, security and justice and taking advantage of new opportunities and chances. First of all, the responsibility for organization and effective implementation of policy cycle laid with COSI whereas Europol's role was limited to produce threat assessments and give inputs for the policy-making process. The policy cycle sought to depart from a loose, often dispersed and fragmented architecture of EU multi-level cooperation in the face of criminal threats towards a centralised COSI-led institutional process engaging EU institutions and agencies in the prevention and fight against serious and organised crime.

The policy cycle reinvigorated the fading ECIM thanks to a flexible formula of EU internal security management and the reduction of the scope of criminal intelligence to serious and international organised crime. It also allowed for diversified methodological solutions more suitable to the complex nature of present dangers and the requirement of pro-active stance with respect to risks and threats to EU internal security.

EU criminal intelligence cooperation - vertical oversight

The European intelligence cooperation mechanisms established by Member States gradually engaged various EU institutions and agencies in information exchange and analysis for the purposes of security, crisis management and public order. Notwithstanding the ever increasing intelligence capabilities of EU bodies, advanced intelligence tradecraft and synergetic connections within the EU, intelligence co-operation is heavily dependent on national strategies, policies and inputs. This dependence is less visible in the strategic dimension of EU intelligence co-operation, where horizontal networks of knowledge-sharing and strategic forecast connect various sources of intelligence and enable the flow of diversified information resources. The vertical setting highlights the preponderance of Member States determined by their national interests as well as political and legal constraints. This is particularly noticeable with regard to oversight mechanisms

worked out by the Member States and implemented in the area of EU intelligence cooperation. The principle of 'sovereign ownership' of information and intelligence products handed over by national authorities for further use by EU institutions and agencies is the cornerstone of EU cooperation. Therefore, information sharing and the delivery of intelligence products is kept in every individual case under the direct supervision of relevant national authorities. The inter-governmental nature of intelligence co-operation, reflected in the configuration of the security field in the EU, is evidenced by the participation of representatives of national governments in the supervision and control of EU agencies belonging to the EU intelligence community. This is especially true with regard to the criminal intelligence and the three agencies operating there: Europol, Eurojust and Frontex.

Under EU law, these agencies area are under review and inspection of governmental bodies established by the Council of the EU or appointed by the Management Board. The Lisbon Treaty provided for the establishment of the Standing Committee on operational cooperation on internal security (COSI). It is responsible for promoting the principles of intelligence-led policing and improving information sharing in the internal security field. COSI monitors developments in the field at the strategic and policy-shaping levels, sets priorities for the agencies and contributes to strategic guidelines adopted by the Council (Council of the EU, 2015).

The EU criminal intelligence is also monitored by representatives of independent national supervisory bodies, making up a joint supervisory authority.This body is created to control the accountability of agencies and have effective supervision over large-scale EU IT systems processing sensitive data for the purposes of EU law, namely the Schengen Information System (SIS II), Eurodac, the Customs Information System (CIS) and the Visa Information System (VIS). It serves to oversee the activities of these agencies and information systems in order to ensure that data is processed properly and in accordance with respective legal provisions. It ensures, in particular, that the rights of the individual are not affected by the storage, processing and use of the data held by the agencies. It examines any difficulty of application and interpretation of the respective legal provisions which may arise during operational activities. It also monitors the

permissibility of the transmission of data originating from the agencies, particularly when third parties are involved.

As far as EU agencies are concerned, the supervisory body is also consulted by the Management Board in matters related to the processing, storing and sharing of information held in the relevant agencies. It can issue opinions and formulate recommendations which, although not binding, are generally taken into account and implemented by the managing institutions of the agencies.

Organization and the assigned tasks may slightly differ among the agencies. Regarding Europol, the Joint Supervisory Board meets at least four times a year and issues public minutes (Europol, 2009). Once a year it conducts a full inspection and, where necessary, additional inspections dedicated to specific issues (Wills et al, 2011, p. 62). Eurojust's JSB meets once in each half year, carries out a full inspectionevery two years with a follow-up visit the next year and may also make regular on-the-spot inspections (Eurojust, 2009; Wills et al, 2011, pp. 62-3). Europol's Management Board appoints an independent Data Protection Officer with access to all the data processed by Europol. The officer is mandated with ensuring the lawful processing of personal data, reporting annually on compliance with the Europol decision and cooperating with the Joint Supervisory Body (Europol, 2009).

Joint supervisory bodies were also established by representatives of the national data protection authorities to oversee the protection of data stored in the EU's large-scale information system. The Schengen Joint Supervisory Authority is in charge of controlling the central unit of the Schengen Information System (SIS II) and ensuring compliance with the relevant provisions on data protection, especially with regard to personal data. The majority of alerts in SIS II concern individuals – third country nationals –and are issued on the grounds of a threat to public policy or public security or to national security(Article 96 CISA). Therefore, the monitoring of SIS II is consistent with general protective rules concerning personal data.

The Visa Information System (VIS) Supervision Co-ordination Group is made up of representatives designated by each of the national supervisory authorities for VIS from each Member State and the European Data Protection Supervisor. It aims to enhance co-operation between the national supervisory authorities and ensure the co-ordinated supervision of VIS and the national systems. It assists the

supervisory authorities in carrying out audits and inspections. It also examines problems with the exercise of independent supervision, especially in the case of the rights of data subjects (VIS, 2013).

Another layer of vertical oversight involves national parliaments. As already mentioned, the national legislatures execute their control and overseeing competences with respect to domestic intelligence services and their foreign linkages. National parliaments remain the centerpieces of democratic control over the intelligence sector in Member States (Herranz-Surrallés, 2014, p. 9). The Lisbon Treaty opened up the possibility for national parliaments to have controlling prerogatives over two EU agencies: Europol and Eurojust. Article 88 TFEU provides that Europol's activities, including the collection, storage, processing, analysis and exchange of information, must be scrutinised by national parliaments (see Abazi, 2014, pp. 1129-30). Likewise Eurojust, in conformity with Article 85 TFEU, is obliged to involve national Parliaments in the evaluation of its activities. However, the treaty stipulates that detailed provisions should be adopted in a regulation by the European Parliament and the Council. Given the sensitivity and complexity of this matter, no regulation has been adopted for the time being. In practice, national parliaments do not enjoy any considerable supervision power regarding Europol and Eurojust.

EU criminal intelligence cooperation - horizontal oversight

The horizontal dimension seems proper for an extensive institutional network characterised by close conections between the entities making up the complex organisational structure. In the case of EU intelligence oversight, the institutional network is not very developed and the relationships between respective entities are not balanced. This is due to the fact that the Council of the EU and the European Council are principally embedded in vertical governmental structures which are quite limited in their monitoring actions at the EU level.

The European Parliament appears to be the institution with strong democratic legitimacy and a vocation to deal with controversial and demanding issues of transparency, control and oversight. The Court of Justice of the EU is limited by the provisions of the EU treaties and is generally excluded from rulings

on intelligence cooperation in the Union. Some specialised bodies are also involved in the oversight and monitoring of the handling of sensitive information, especially personal data. Although their impact on the European intelligence community is marginal, it is worth presenting briefly their oversight competences.

The European Data Protection Supervisor (EDPS) was established in 2004 to uphold privacy rules when personal data is processed by the EU institutions and bodies in the course of their duties, including for intelligence purposes. The European Ombudsman conducts inquiries in cases of alleged maladministration by EU agencies and bodies, which might concern, amongst other things, public access to documents (De Moor &Vermeulen, 2011, p. 387). Another horizontal body is the Article 29 Data Protection Working Party set up under the Directive 95/46/EC on the protection of individuals with regard to theprocessing of personal data and on the free movement of such data (European Parliament and the Council of the EU, 1995). It brings together representatives of the national data protection authorities, the EDPS and the European Commission. It is an advisory body promoting the uniform application of the general principles of data protection and providing expertise with regard to the processing of personal data and privacy in the EU.

The European Parliament occupies a prominent place in the EU system of horizontal oversight, especially following the Lisbon Treaty reform. Its oversight competences have definitely been widened formally and strengthened in practice, although they still lack sharpness and are constrained by the exisiting regulations of access to classified information.

As far as criminal intelligence is concerned, with the introduction of an ordinary (co-decision) legislative procedure to the whole area of freedom, security and justice (with single exemptions), the European Parliament has gained more influence over the performance of agencies involved in EU criminal intelligence cooperation. This was particularly important in the comparative historical perspective which presented parliamentary oversight as an underdeveloped area hampered by ‘the logic of intergovernmentalism favouring the executives over the legislatives’ (Puntscher Riekmann, 2008, p. 32).

However, this new capacity has still to be considered in the conditional tense. Provisions of the Lisbon Treaty concerning the extended competences of the

European Parliament regarding the scrutiny and evaluation of criminal intelligence agencies, namely Europol and Eurojust, still await their effective fulfilment. Article 88 of the TFEU stipulates that scrutiny of Europol's activities, including the collection, storage, processing, analysis and exchange of information, in particular that forwarded by the authorities of Member States or third countries or bodies, must be conducted by the European Parliament.

The new regulation on Europol (European Parliament and the Council of the EU, 2016), adopted by the Council in May 2016 (with effect from 1 May 2017), provides in Article 51 for the establishment of a Joint Parliamentary Scrutiny Group (JPSG). It will be composed of members of national parliaments and of the 'competent committee' of the European Parliament, ie the LIBE (Civil Liberties, Justice and Home Affairs) Committee. The JPSG's task is to 'politically monitor Europol's activities in fulfilling its mission [...]. It is entitled to invite the Chairperson of the Management Board, Europol's Executive Director or their Deputies to discuss matters relating to the activities of the agency.

The JPSG is authorised to receive for information purposes and under discretion and confidentiality 'relevant documents' including 'threat assessments, strategic analyses and general situation reports relating to Europol's objective as well as the results of studies and evaluations commissioned by Europol.'However, no sensitive non-classified materials can be automatically delivered to JPSG members. It will be subject to rules on discretion and confidentiality and on the protection of sensitive non-classified information established by Europol in conformity with Decision 2013/488/EU on the protection of EU classified information, ensuring an equivalent level of protection. In practice, the parlamentarians may be easily denied of access to the most relevant information and data held by Europol.

Unlike Europol, the parliamentary impact on evaluation of Eurojust activities still lacks detailed provisions. According to Article 85 TFEU, the European Parliament and national parliaments shall be involved in the evaluation of Eurojust's activities. No specific arrangements were adopted for the time being, although the European Commission has already presented several proposals in this regard. In 2013 it presented a proposal for new regulations reconstituting the agency. Interestingly, detailed provisions concerning parliamentary scrutiny differ

substantially between both agencies, highlighting the essential distinction between 'evaluation' (Eurojust) and 'scrutiny' (Europol). Both agencies are subject to general evaluation requirements including the appearance of the heads of the agencies and chairpersons of the Management Boards before the European Parliament (taking into account the obligation to observe discretion and confidentiality). Eurojust will be obliged to transmit to the European Parliament and national parliaments the results of studies and strategic projects elaborated or commissioned by Eurojust as well as working arrangements concluded with third parties, subject to rules on confidentiality.

In contrast to Europol and Eurojust, Frontex is not explicitly mentioned in the Treaty on the functioning of the European Union in the context of scrutiny or evaluation of its activities. The European Parliament, then, executes general oversight but it is deemed quite insufficient for the effective supervision of the management of sensitive data, particularly for the purposes of risk analysis, threat assessment, situational and pre-frontier intelligence pictures. This relates particularly to the controversy over processing the personal data of certain groups of the migrant population (returnees, 'facilitators', suspected human traffickers) where Frontex used to apply the secrecy rule (Carrera, 2007, p. 14). Likewise, the draft regulation on the European Border and Coast Guard (EBCG) replacing Frontex does not rearrange rules on information sharing, excluding intelligence exchange despite provisions empowering the EBCG to prevent cross-border crime including facilitation of irregular illegal immigration, trafficking in human beings and terrorism.

The European Parliament also has an important competence in the sphere of the EU's external relations. According to the Article 218 of the TFEU, the consent of the European Parliament is required for the conclusion of international agreements by the EU that cover fields to which ordinary legislative procedure applies. Therefore, the European Parliament exercises control over the international commitments negotiatied by the Commission and made by the Council on behalf of the European Union. Any international agreement adopted by the EU with regard to information exchange and data sharing must be approved by the European Parliament. The cooperation between the European Union and the United States in information exchange and intelligence sharing contained specific formal

and informal procedures, mechanisms and tools. The cases of PNR, SWIFT and 'Umbrella' agreements have been particularly illustrative of determination and engagement on the part of the European Parliament. Given the volume and sensitivity of data and information exchanged under established arrangements, EU institutions have faced a serious dilemma when evaluating these working arrangements from the perspective of fundamental rights and civil liberties, namely privacy, personal data protection and remedies.The European Parliament has been particularly active and – as already noted – determined to prevent EU citizens from any possible misuse or abuse of their privacy for the sake of security measures adopted during the 'war on terror'.

The European Parliament's oversight should also take into account the activity of its individual members (MEPs), shown not only during debates in the dedicated parliamentary commissions and at the general assembly, but also in the form of questions addressed to EU institutions performing vertical oversight and administrative control over EU intelligence bodies. These questions not only looked for additional information and explanation of certain aspects of EU intelligence cooperation but also tested the scope of the sensitivity of information possessed by EU institutions, mainly the Council and the Commission, and the framework of its availability under applicable EU law.

Judicial control over EU agencies and bodies involved in intelligence-led activities has remained a source of concern, mostly due to certain exceptions and exclusions of operational activities from the control executed by the Court of Justice (Gless, 2002; Wagner, 2006; De Moor &Vermeulen, 2010). According to the relevant provisions of the Lisbon Treaty (Article 276 TFEU), the Court is not authorised to review the validity or proportionality of operations carried out by the police or other law-enforcement services of a Member State or the exercise of the responsibilities incumbent uponMember States with regard to the maintenance of law and order and the safeguarding of internalsecurity (Article 276 TFEU). Despite extending the competences of the Court of Justice in the Lisbon Treaty, it still has a limited and fragmented jurisdiction over internal security and criminal justice in the EU (Wolff, 2012, p. 67).

Conclusions

The emergence and development of criminal intelligence had its roots in the very phenomenon of organised crime reflecting a dynamic process of transition from individual locally-based criminality to transnational organised serious crime with powerful resources and the global reach. The European Union's institutions and Member States' relevant authorities reached in the mid-2000s a critical level of common awareness and mutual understanding with respect to the gravity of dangers posed by terrorist networks and transnational organised criminal groups. Strong political impulse sent by the European Council in the aftermath of the terrorist act in Madrid in 2004, enhanced in the Hague Programme, was orchestrated with the growing activeness and organizational stabilization of EU agencies in the field of security and justice: Europol and Eurojust.

EU institutions competent in the field of criminal justice and home affairs took over responsibility for adopting legal instruments and measures with regard to criminal intelligence. As mentioned above, the Council decided to put forward the ECIM and to integrate this project with the policy cycle for organised and serious crime with the aim to improve efficiency of proactive strategy of tackling the problem of organised criminality through a comprehensive threat assessment and translation of identified goals into operational activities.

The effective use of criminal intelligence remains the domain of national law enforcement services and their ability to prevent and combat criminal groups. However, efficiency of criminal proceedings should take into account not only the operational aspects of law enforcement in a given Member State but also some organisational prerequisites emerging at supranational level and embedded in general strategies and operational plans adopted in a consensual way.

The practice of oversight and accountability in the EU has engendered mixed responses. The juxtaposition of vertical and horizontal dimensions indicates that forms and means of oversight seem to be rather fuzzy due to the deficit of hierarchical assumptions underpinning accountability mechanisms and substantial gaps in the institutional setting of horizontal oversight at the EU level. Müller-Wille observed, as early as the mid-2000s, that 'The main deficits in terms of democratic accountability of the European intelligence community are located at the national

level. This is where the collection of intelligence takes place, the main risk of abuse of state powers lies, and the greatest threats are posed to civil liberties.' (Müller-Wille, 2006, p. 125). Indeed, the principle of originator control is the critical determinant of intelligence oversight in the EU, hampering efforts to strengthen the independent control and supervision of information management and intelligence sharing in the EU security fields (Walsh, 2006, p. 635; Abazi, 2014, p. 1122).

National intelligence services are obliged to observe the rules and principles of democratic oversight in their countries and follow guidelines for international co-operation (Born, Leigh & Wills, 2015, pp. 84-8; Bigo et al, 2015). When it comes to practical activities in the international dimension, they also become subject tomonitoring and evaluation performed by transnational institutions co-ordinating co-operation in the area of information exchange and intelligence sharing. However, as Wetzling (2009, p. 108) noted, 'concerted intelligence activities escape the remit of national accountability forums, whilst not being absorbed by existing European accountability forums either.' Effective EU oversight is undermined by a deficit of European public authority. Moreover, it does not cover a relatively wide field of semi-official intelligence co-operation, especially on counter-terrorism and the fight against crime, such as the Berne Club, the Police Working Group on Terrorism or, to a certain extent, the G6 Group.

On the other hand, robust intelligence co-operation requires an adequate level of discretion. This can limit the oversight capacities of transnational bodies yet it does not necessarily curb accountability of institutions involved in intelligence sharing. As Curtin, Mair and Papadopoulos argue (2010, pp. 936-7), openness has not always been regarded as an obvious element of government. Accountability cannot be simplistically reduced to openness. The oversight functions performed by the European Parliament emphasise the transparency of EU agencies and access to all available information concerning intelligence co-operation at the EU level. Abazi (2014, p. 1132) rightly observes that 'The new oversight role of the European Parliament is multifaceted and highly dependent on receiving information, either in the form of reports or through direct questions and statements'. However, the European Parliament has been constantly separated from sensitive information and pre-processed intelligence delivered by intelligence

agencies from Member States. Governments still have plenty of room to manoeuvre with regard to formal oversight and accountability procedures and mechanisms. Their strong position vis a vis EU oversight institutions and bodies means that transnational intelligence co-operation and information exchange can barely escape the existing national mechanisms of control and evaluation.

Evaluation and assessment of the scope and content of intelligence production in the EU is a joint undertaking of EU agencies and units and respective national services. Institutional oversight includes a set of measures, procedures and mechanisms generated at the intersection of separate ambits of intelligence management and tradecraft practiced in the EU by its agencies and Member States. As a result, the oversight and accountability of EU criminal intelligence cooperation are subject to disaggregated policy arrangements established at different levels of the co-ordination of knowledge management practices in the realm of EU internal security.

Bibliography:

Abazi, V. (2014). The Future of Europol's Parliamentary Oversight: A Great Leap Forward?. *German Law Journal*, 15(6), 1121-1143.

Baker, J.A. (2008). Intelligence Oversight. *Harvard Journal on Legislation*, 45(1), 199-208.

Benz, A., Harlow, C. and Papadopoulos, Y. (2007). Introduction. *European Law Journal*, 13(4), 441–446.

Bigo, D. et al. (2015). *National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges*. CEPS Paper in Liberty and Security No. 78. Brussels: CEPS.

Bono, G. (2006). Challenges of Democratic Oversight of EU Security Policies. *European Security*, 15(4), 431-449.

Born, H., Leigh, I. and Wills, A. (2015). *Making International Intelligence Cooperation Accountable*. Geneva: EOS-DCAF.

Bossong, R. & Rhinard, M. (2013) The EU Internal Security Strategy. Towards a More Coherent Approach to EU Security?. *Studia Diplomatica*. LXVI (2). p. 45-58.

Bovens, M. (2010). Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism. *West European Politics*, 33(5), 946-967.

Bures, O. (2006). EU Counterterrorism Policy: A Paper Tiger? *Terrorism and Political Violence*, 18(1), 57-78.

Caparini, M. (2007). Controlling and Overseeing Intelligence Services in Democratic States. In H. Born and M. Caparini (eds), *Democratic control of intelligence services: containing rogue elephants*. Aldershot - Burlington, VT: Ashgate.

Carrera, S. (2007). *The EU Border Management Strategy. FRONTEX and the Challenges of Irregular Immigration in the Canary Islands*. CEPS Working Document No. 261. Brussels: CEPS.

Council of the EU (2006a) Comprehensive Operational Strategic Planning for the Police (COSPOL). Doc. 5859/4/06 REV 4 LIMITE (10th October).

Council of the EU (2006b) Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. *Official Journal of the European Union*. L 386 (29th December).

Council of the EU (2010a) *Internal Security Strategy for the European Union. Towards a European Security Model*. Brussels: General Secretariat of the Council.

Council of the EU (2010b) Council conclusions on the creation and implementation of a EU policy cycle for organised and serious international crime, 3043rd JUSTICE and HOME AFFAIRS Council meeting, Brussels, 8 and 9 November 2010. At https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/117583.pdf, accessed 12 November 2010.

Council of the EU (2010c) Expert group – EU Policy cycle. Doc. 11814/10 LIMITE (5th July).

Council of the EU (2010d) EU Policy Cycle. Doc. 12657/1/10 REV 1 (3rd September).

Council of the EU (2012) *Serious and Organised Crime Threat Assessment (SOCTA) - Methodology*. Doc. 12159/12 (4th July).

Council of the EU (2015). *Renewed European Union Internal Security Strategy Implementation Paper*, doc. 10854/15, Brussels, 14 July.

Curtin, D., Mair, P. and Papadopoulos, Y. (2010). Positioning Accountability in European Governance: An Introduction. *West European Politics*, 33(5), 929-945.

De Moor, A. and Vermeulen, G. (2010). The Europol Council Decision: Transforming Europol into an Agency of the European Union. *Common Market Law Review*, 47(4), 1089–1121.

De Moor, A. and Vermeulen, G. (2011). Europol and Eurojust. In A. Wills et al., *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*. Brussels: European Parliament.

Duke, S. (2006). Intelligence, security, and information flows in CFSP. *Intelligence and National Security*, 21(4), 604–630.

Erskine, T. (2004). 'As Rays of Light to the Human Soul'? Moral Agents and Intelligence Gathering. *Intelligence and National Security*,19(2), 359-381.

Eurojust (2009). Act of the Joint Supervisory Body Of Eurojust of 23 June 2009 laying down its rules of procedure. *Official Journal of the European Union*, C 182, 7 July.

European Commission (2004) Communication from the Commission to the Council and the European Parliament. Towards enhancing access to information by law enforcement agencies. Doc. COM (2004) 429 final (16th June).

European Council (2004) The Hague Programme: Strengthening Freedom, Security and Justice in the European Union. *Official Journal of the European Union* C 53 (3 March).

European Council (2010) 'The Stockholm Programme – An open and secure Europe serving and protecting the citizens', *Official Journal of the European Union*. C115 (4th May).

Europol (2009). Act no 29/2009 of the Joint Supervisory Body of Europol of 22 June 2009 laying down its rules of procedure. *Official Journal of the European Union*, C 45, 23 February.

European Parliament and the Council of the EU (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*, L 281, 23 November.

European Parliament and the Council of the EU (2016). Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. *Official Journal of the European Communities*, L 135, 24 May.

Gill, P. and Phythian, M. (2012). *Intelligence in an Insecure World,* 2nd ed. Cambridge: Polity Press.

Gless, S. (2002). What Kind of Judicial Control do the New Protagonists Need?: The Accountability of the European Police Office (Europol). In G. de Kerchove and A. Weyemberg (eds), *L'espace pénal européen: enjeux et perspectives*. Bruxelles: Editions de l'Université de Bruxelles.

Grant, R.W. and Keohane, R.O. (2005). Accountability and Abuses of Power in World Politics. *American Political Science Review*, 99(1), 29–44.

Herman, M. (2004). Ethics and Intelligence after September 2001. *Intelligence and National Security*,19(2), 342-358.

Herranz-Surrallés, A. (2014) *Parliamentary Oversight of EU Foreign And Security Policy: Moving Beyond the Patchwork?*. ISPI Analysis No. 230. At http://www.ispionline.it/sites/default/files/pubblicazioni/analysis_230_2013.pdf; accessed 15 March 2015.

Horgby, A. & Rhinard, M. (2013) *The EU's Internal Security Strategy: Living in the Shadow of Its Past*. Occassional Paper no. 24. Stockholm: The Swedish Institute of International Affairs.

Keohane, R.O. (2006). Accountability in World Politics. *Scandinavian Political Studies*, 29(2), 75-87.

Leigh, I. (2011). Accountability and intelligence cooperation: framing the issue. In H. Born, I. Leigh and A. Willis (eds), *International Intelligence Cooperation and Accountability*. Abingdon - New York: Routledge.

Leigh, I. (2015). *Fostering cooperation and exchange of best practices between intelligence oversight bodies in the EU*. Remarks to the Conference on the Democratic oversight of Intelligence services in the European Union, Brussels, 28 May. At https://polcms.secure.europarl.europa.eu/cmsdata/upload/5351c536-5683-40ab-b639-0a386f7ae04c/Ian_Leigh_Durham_University.pdf; accessed 22 June 2015.

Mann, S., Nolan, J. and Wellman, B. (2003). Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance & Society*,1(3), 331-355.

Müller-Wille, B. (2006). Improving the democratic accountability of EU intelligence. *Intelligence and National Security*, 21(1),100-128.

O'Donnell, G. (1994). Delegative Democracy. *Journal of Democracy*, 5(1), 55-69.

Pastor, R.A. (1999). The Third Dimension of Accountability: The International Community in National Elections. In A. Schedler, L. Diamond and M.F.Plattner (eds), *The Self-Restraining State. Power and Accountability in New Democracies*. Boulder, CO - London: Lynne Rienner Publishers.

Puntscher Riekmann, S. (2008). Security, Freedom and Accountability: Europol and Frontex. In E. Guild and F. Geyer (eds), *Security versus Justice? Police and Judicial Cooperation in the European Union*. Aldershot – Burlington, VT: Ashgate.

Sepper, E. (2010). Democracy, Human Rights, and Intelligence Sharing. *Texas International Law Journal*, 46(1), 151-207.

Trechsel, A.H. (2010). Reflexive Accountability and Direct Democracy. *West European Politics*, 33(5), 1050-1064.

UK Presidency (2005) A European Criminal Intelligence Model. Paper issued by the 2005 UK Presidency of the EU.

US Department of Justice (2003)*National Criminal Intelligence Sharing Plan*. Washington, DC: US Department of Justice, Office of Justice Programs. At

http://www.cops.usdoj.gov/files/ric/CDROMs/LEIntelGuide/pubs/National_Criminal_Intelligence_Sharing_Plan.pdf; accessed 14 February 2016.

Van Buuren, J. (2013). From Oversight to Undersight: the Internationalization of Intelligence. *Security and Human Rights*, 24(3-4), 239-252.

VIS (2013). Visa Information System (VIS) Supervision Coordination Group Rules of Procedure Brussels, 11 April. At https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/VIS/13-04-11_VIS_Supervision_Coordination_Group_RoP_EN.pdf; accessed 16 May 2015.

Wagner, W. (2006). Guarding the guards. The European Convention and the communitization of police co-operation. *Journal of European Public Policy*, 13(8), 1230-1246.

Waldrauch, H. (1998). *Institutionalizing Horizontal Accountability. A Conference Report*. Political Science Series No. 55. Vienna: Institute for Advanced Studies.

Walsh, J.I. (2006). Intelligence-Sharing in the European Union: Institutions Are Not Enough. *Journal of Common Market Studies*, 44(3), 625-643.

Wetzling, Th. (2009). European intelligence cooperation and accountability. In: S. Gustavsson, Ch. Karlsson and Th. Persson (eds), *The Illusion of Accountability in the European Union*. London - New York: Routledge.

Wills, A. et al. (2011). *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*. Brussels: European Parliament.

Wolff, S. (2012). The New EU's Internal Security Architecture Implementation Challenges. In F. Laursen (ed), *The EU's Lisbon Treaty. Institutional Choices and Implementation*. Farnham - Burlington, VT: Ashgate.