UACES 43rd Annual Conference

Leeds, 2-4 September 2013

www.uaces.org

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

Intelligence tradecraft and the pre-crime approach to EU internal security governance

Paper to the UACES 43rd Annual Conference, Leeds, 2-4 September 2013

Abstract

EU internal security policy has been in recent years progressively focused on prevention of threats and risks. The 2010 Internal Security Strategy for the EU highlighted the need for 'prevention and anticipation' conceived as a proactive intelligence-led approach to EU internal security. A pre-crime framework has been widely applied in fields like security studies, police science, criminology, ethics, political sociology and political geography, owing to its inherent explanatory power. The core element of pre-crime approach is the selection and identification of the most probable among abstract risks and dispersed threats, and the profiling, or sorting out, of particular social groups or individuals posing presumably imminent threats. This paper aims at inserting the concept of intelligence tradecraft into the pre-crime analytical framework and verify the usefulness of such an approach to the study of EU internal security governance. The paper will focus on 'intelligence process' and 'intelligence product', i.e. how the stakeholders of EU internal security policy construct, modify and develop 'products' allowing for a better risk management and threat assessment in the context of precautionary and anticipatory attitudes towards EU security governance.

Keywords

Anticipation – intelligence - police co-operation - pre-crime approach - security

Introduction

EU internal security policy has been in recent years progressively focused on prevention of threats and risks. The 2010 Internal Security Strategy for the EU highlighted the need for 'prevention and anticipation' conceived as a proactive intelligence-led approach to EU internal security. The long history of terrorist activities and explosions of violence in Europe has taught the state authorities and societies that preventing surprise attacks requires substantial forecasting and should be the main task of intelligence services.

The persistence of organised crime in different forms produces constant threat to security and prosperity of EU citizens. Global networks and communication systems facilitate proliferation of risks which are no longer confined geographically. In these circumstances security policies formulated, arranged and performed by the governments and supranational institutions are increasingly concentrated on detection, identification and deactivation of potential and immediate threats in order to safeguard the public space through the mechanisms of early warning, prevention and anticipation.

In the face of the growing belief in technologies of surveillance and control and the feeling of helplessness of traditional human-based methods of maintaining public order, the broadening application of the concept of intelligence is a feature of today's world. Obviously enough, it raises protests and criticism on the part of mainstream intelligence officials and scholars who are afraid of the overload of information, declining standards of intelligence activities, the widening margins of error in intelligence analysis, and even devastating effects for decisionmaking and democratic governance (Agrell 2002). This also gives rise to concerns regarding fundamental rights, citizens' freedoms and civil liberties. In the debate on the relationship between liberty and security, most often focused on the price that contemporary societies have to pay in exchange of the protective shield set by their states (Anderson and Apap 2002; Waldron 2003; Berman 2004; Solove 2004, 2011; Balzacq and Carrera 2006; Huysmans 2006; Northouse 2006; Bigo and Tsoukala 2008; Meisels 2008; Bobbitt 2008, Aradau 2008), the dilemma of how government may govern and intervene in our future society is of particular relevance. This question is fundamental to risk assessment, crime prevention or counter-terrorism, and it has acquired the growing importance in the crafting of methodology for the study of contemporary security governance.

The apparent dichotomy 'liberty vs security' also encouraged reflection on the temporal dimension of security, especially in its future tense or in the perspective of threats to come and chances to avoid them. All in all, the core element of the ongoing discussion was the selection and identification of the most probable among abstract risks and dispersed threats, and the profiling, or sorting

out, of particular social groups or individuals posing presumably imminent threats. In terms of security governance, it has to involve specific modes, techniques and tools of data processing and knowledge management in the context of precaution and anticipation. This led, almost naturally, to the thinking about security as a process of active prevention of criminal offences from being committed and the preemption of terrorist attacks and other serious criminal acts or imminent evidences of military activities and hostilities before they take place (Litwak 2002-03; Kegley and Raymond 2003; Blinken 2003-04; Feinstein and Slaughter 2004; Lee 2004; Luban 2004; Ackerman 2006; Daalder 2007; Shue and Rodin 2007; Bzostek 2008; Amoore and De Goede 2008; Guiora 2008). This is how the pre-crime approach was born.

A pre-crime framework has already been applied in fields like security studies (McCulloch and Pickering 2009; Mythen and Walklate 2010; De Goede 2008, 2011; Aradau and van Munster 2012; Bigo 2012), police science (Kölbel and Selter 2010; van Brakel and De Hert 2011), criminology (Fitzgibbon 2004; Hebenton and Seddon 2009; Zedner, 2007, 2010; Botterhuis, van der Duin, de Ruijter and van Wijck 2010), public policy (Jablonowski 2006; Fuerth 2009; DeLeo 2010), economics (Glenn 2013), ethics (Krahn, Fenton and Meynell 2010), political philosophy (Poli 2010), political sociology (Huiskamp 2004; Aradau and van Munster 2011), cultural studies (Cooper 2006; Grusin 2010) and human geography (Weber 2005; Anderson 2010a, 2010b; Wortley and McFarlane 2011; Adey and Anderson 2012). Such a widespread application of this concept may be owing to its inherent explanatory power, especially with regard to the tendency of shifting the horizon of insecurity and uncertainty as far away as possible from agents responsible for law, order, and security. In a similar vein, the pre-crime approach may be deployed in the face of security threats, which must be countered before a crisis occurs, due to their substantial gravity and large-scale effects. This also applies in the form of a 'what-if' scenario before a crisis occurs or before a crime is committed, and the danger to state and society has materialised. Both of these uses in the field of security studies have a common root: a political responsibility for protecting the populace must be maintained for the longest period possible, in order to minimise the 'post-crime' costs of public insecurity, crisis management and criminal proceedings.

EU internal security governance, measured by the legitimacy and efficiency of means, instruments, methods and techniques involved in it, has increasingly depended on the capability of decision makers at both the EU and national levels to utilize the pre-crime approach for maximum effect. As Ericson wrote, 'There is also a new sanctioning of responsibilities which escapes reference to anything but uncertainty: as the person responsible for precautionary measures, the designated agent is judged not only by what she should known but also by what she should have expected' (Ericson 2007, 24). Thus, the relevance of pre-crime has political origins, given that it stems from a growing tension between the state's limited

security capabilities and society's 'maximum security' needs and demands. The effect of such reasoning was to recognise that both prediction and risk management are entirely feasible and objective (Zedner 2007, 267-68). Apparently, it seemed to be a technical and organizational matter how to extract elements of threats, risks, perils and hazards from the continuously emerging security landscape.

Techniques and practices which incorporate pro-active, pre-emptive elements have been noted in criminal justice for decades. Nevertheless, their widespread presence in policing, security governance, civil protection and forensics is largely a phenomenon of recent times. The rapid development of technologies and tools which allow for virtually planning security, such as the simulation of credible threats, risk assessment, criminal profiling and the 'stealth' management of identity, has accelerated and facilitated the search for solutions linking prevention to prediction and pre-mediation (Carroll-Mayer, Fairweather and Stahl 2008; Hildebrandt and Gutwirth 2008; Neyland 2009; Bohm and Mason 2010; Gutwirth, Poullet and De Hert 2010. This 'precautionary logic' (Ericson 2007, 21-24) inevitably led to increasing involvement of the state security apparatus in threat assessment, early warning systems, and intelligence gathering. The pre-crime approach was associated with a capacity for 'accurately predicting threats through intelligence rel[ying] on accurate information on the variables associated with increased threat' (McCulloch and Pickering 2009, 635).

The application of intelligence in the area of internal security, home affairs and criminal justice raises certain methodological reservations. There is a need for a practical and comprehensive conceptualization of intelligence which could be applicable to both internal security and law enforcement and thereby validate feasibility of the pre-crime framework for analysis adopted in this paper. Criminal intelligence analysis is a concept which seems to match intrinsic features of the twenty-first-century global organized criminal structures. Moreover, this concept was formulated by the UN Office on Drugs and Crime as a tool for intelligence analysts and experts on criminal information and intelligence databases (UNODC 2011). It permits law enforcement services to elicit a pro-active response to threats and risks posed by organized criminal activities. The steps taken in the past years by the European Union institutions and agencies, especially the European Council and the Council, as well as Europol and Frontex, definitely lead towards intelligence-led policing, pro-active law enforcement and intelligence-driven situation assessment. Criminal intelligence analysis underpins EU internal security governance in terms of acquiring a knowledge and foreknowledge about threats, challenges, risks and working out long-term solutions to tackle them in the most effective way.

This paper also inserts the concept of intelligence tradecraft into the pre-crime analytical framework and verify the usefulness of such an approach to the

study of EU internal security governance. The paper will focus on 'intelligence process' and 'intelligence product', i.e. how the stakeholders of EU internal security policy construct, modify and develop 'products' allowing for a better risk analysis and threat assessment in the context of precautionary and anticipatory attitudes towards EU security governance. In the case of EU internal security, intelligence tradecraft, conceived as organizational capability enabling the emergence of synergies between EU agencies and bodies involved in information gathering, processing and exchange, is an important factor determining success or failure of security governance.

The thesis developed in this paper is that a pre-crime approach, built on enhanced prevention and effective anticipation achieved through horizontal coordination at the EU level, needs a tailor-made genuine intelligence tradecraft. This is a prerequisite to the development and reinforcement of a legitimate, effective and prospective model of internal security governance in the EU. Consequently, an EU intelligence tradecraft should be put into practice in order to consolidate the Union as an accountable 'security provider'. Hitherto activities taken by EU institutions and agencies as well as the Member States have shown that knowledge management, data processing and intelligence analysis are still the domain of national agencies although the EU has confirmed its increasing capabilities in this area. The choice of a pre-crime framework is a strategically motivated option exercised at EU level as a subsidiary mechanism with regard to enhanced, technologically driven surveillance and control by national security and law enforcement services. It is followed by the development and improvement of methods, instruments and skills making up the EU criminal intelligence tradecraft.

The sections of the paper proceed as follows: In section one, the concept of intelligence tradecraft is explained and synthesised on the basis of mainstream intelligence literature. Next, the shift in EU internal security policy to an anticipatory approach, is explained as a necessary exposition of legal and institutional prerequisites for creating a pre-crime framework. This section also highlights preventive aspects of security strategies and political guidelines. Section three presents EU criminal intelligence model as a part of an EU-wide policy cycle for organised and serious international crime. Section four discusses risk analysis model on the example of Frontex. Next section elaborates on threat assessment methodology, particularly that adopted by Europol in the framework of the serious and organised crime threat assessment. The conclusions focus on the argument that the European Union has to develop and proliferate a common intelligence tradecraft in order to strengthen the pre-crime approach within a model of security governance due to the relative weakness of alternative solutions available at the EU level of cooperation in the field of internal security.

What is intelligence tradecraft?

In the study of intelligence, the notion of 'tradecraft' is applied to describe the way in which intelligence becomes a commodity exchanged between agencies in order to gain a competitive advantage. According to a strict definition of "tradecraft", it is referred to "the techniques of the espionage trade, or the methods by which an agency involved in espionage conducts its business." (Lemer and Lemer 2004, 167). Tradecraft may be also conceived as a skill-set necessary for acquiring information and converting it into intelligence.

The traditional notion of tradecraft was associated with "the ways in which an intelligence officer arranged to make contact with an agent, the means by which the agent passed on information to the officer, the method for paying the agent, and the many precautions and tactics of deception applied along the way" (Lemer and Lemer 2004, 167).

Nowadays the craft of intelligence has to take into account the change in targets of intelligence – from states (mostly global and regional powers) and international governmental organizations to non-state actors, terrorist organizations, transnational criminal networks (Treverton 2009, 15-16). In the face of present-day problems, challenges and threats, tradecraft seeks to combine classical methods that an intelligence officer (agent, expert, analyst) uses in the performance of his or her duties with technologically-driven knowledge management tools making use of sophisticated machinery. Tradecraft then is a combination of individual abilities, talents and skills as well as common sense, experience and hunch with norms, procedures, guidelines, methods, organizational structures and – last but not least – technical and financial capabilities. The two dimensions of tradecraft: subjective and objective, correspond with another division. Tradecraft may be also considered in two aspects: operational and analytical. The former puts emphasis on practical skills and abilities to convert available information and data into tactical intelligence and translate intelligence products into operational support stuff. The latter refers to the ability of processing raw information and available data along strategic guidelines and generalizations that will support and stimulate the performance of intelligence services.

The craft of intelligence is expressed in the intelligence process that produces insights for policymaking. Any intelligence tradecraft is subject to a model of sequential activities allowing for a systemic, comprehensive and logical gathering and processing of information and data. The so-called intelligence cycle stimulates specific cognitive attitudes and behaviours in intelligence officers that have a direct impact on quality and quantity of intelligence products. It also puts a kind of order into the whole inventory of methods, techniques and state-of-the-art

technologies used to produce intelligence. The intelligence cycle is a process of developing raw information and unrefined data into finished intelligence for the use of the authorized customers (policymakers). Writ large, it includes tasking, collecting, processing, analyzing, and disseminating intelligence. It starts with identifying customer needs. On the basis of these requirements, planning and direction is made in order to manage effectively the entire cycle. The next step is collection and acquisition of information and data from variegated sources. Then processing and exploitation takes place and consists in converting the vast amount of information collected into a form usable by analysts. The next stage refers to analysis, evaluation and integration of available data with the aim of preparing finished intelligence products. Finally, at dissemination stage, intelligence products reach the consumers whose started the cycle. Quite often, 'soft' intelligence products, devoid of confidential or restricted information, are made available to the public as a way to raise its awareness and stimulate resilience to the identified threats (Steele 2002; Xu 2007; George 2008; Lowenthal 2008).

At every stage of the intelligence cycle, the tradecraft has to take into account the disciplines of intelligence. This is important for technical and organizational reasons, since every discipline requires specific elements of the craft of intelligence and delivers specific input to the cycle of intelligence analysis. Human intelligence (HUMINT) relies on interpersonal contacts, be it open or covert, conducive to certain information in possession of a person or a group of persons. Signal intelligence (SIGINT) involves remote acquiring and transmission of information and data through technologically advances high-capacity electronic devices. Imaginery intelligence (IMINT) consists in obtaining and processing of photographs and other types of imagery. Measurement and signature intelligence (MASINT) is an analysis of physical attributes of certain objects, or targets, facilitating subsequent identification and/or measurement of these objects. Open-source intelligence (OSINT), growing in popularity and utility, refers to a broad array of information and sources that are generally available, including information obtained from the media, professional and academic records, and publicly available data. Social media intelligence (SOCMINT) is a relatively new discipline, responding to the rapid virtualization of social communication and the expansion of cyberspace. SOCMINT is intelligence derived from social media through scanning, measurement and analysis of information shared by the users of these media (Steele 2002, 18-21; Richelson 2012; Omand, Bartlett and Miller 2012).

In every one of the above mentioned disciplines, intelligence analysis is the core of the tradecraft. Analytical tradecraft is the term used to describe the principles and tools used by analysts to instill rigour in their thinking and prevent cognitive biases from skewing their analytic judgments. Through the use of structured analytic techniques, analysts make their argumentation and logic more transparent and subject to further investigation. In analysis, tradecraft comprises the cognitive and methodological tools and techniques used by analysts to gather

and organize data, interpret their meaning, and produce judgments, insights and forecasts for policymakers and other users of finished intelligence products. Analytic performance is an indicator, a sort of litmus test, for the whole intelligence community as the provider of insights, anticipatory and preventive guidelines. When effective and successful, it consolidates the analytical tradecraft, validates the intelligence cycle and legitimises the entire analytic community. In case of mistakes or failures, it triggers off a chain of substantial changes affective the whole tradecraft practiced by the intelligence community. Johnston observed that: 'The adoption of the word "tradecraft" demonstrates the analytic community's need to create a professional identity separate and unique from other disciplines but tied directly to the perceived prestige and cachet of intelligence operations' (Johnston 2005, 18).

The focus on analysis and production of intelligence gives up the traditional feature of intelligence tradecraft as the set of methods, skills and instruments implemented in operations rather than analytic work (Johnston 2005, 17). However, recent changes in intelligence theory and practice suggest the increasing role of analytical aspects and cognitive abilities of individuals participating in the intelligence cycle. 'Software' instead of 'hardware' predominates nowadays the craft of intelligence. Failures noticed in recent years proved that intelligence community awash in data acquired by intelligence machinery may feel exposed to the risk of overload and pressure from customers awaiting tailor-made solutions to the identified security dilemmas. The syndrome of 'big data' flowing into every area of the globe is perceived as a source of escalating problems and dilemmas of political, technical, financial, organizational, legal and ethical nature.

Therefore, the future orientation in intelligence tradecraft is analysis-centric instead of collection-centric (Treverton and Gabbard 2008, 44). However, both approaches should be well balanced and tied by synergetic connections. This is a demanding task for governments, national intelligence communities and transnational institutions and agencies. The case of the European Union is no exception.

Strategic Dimension of the Pre-Crime Approach to EU Internal Security

Given its responsibility for providing security for both individual states as well as citizens within the area of freedom, security, and justice, the European Union has been attempting to formulate a viable and cogent response towards the security challenges facing its Members since the end of the 20th century. In the wake of the tragic events of 11 September 2001, counterterrorism policy began to occupy almost the entire agenda for cooperation within the EU Justice and Home Affairs (Winn 2003, 154-155; Occhipinti 2003; Wiener 2008; Friedrichs 2008; Deflem

2010; Argomaniz 2011). Despite this change in focus, however, the activities of EU institutions and Member States were still following intergovernmental arrangements, focused on a reactive approach to threat management which underlined its limited preventive capabilities. In effect, decades of confrontation with various forms of terrorism experienced by several Member States gave rise to practices and patterns which effectively precluded an anticipatory intervention at the EU level.

Developments in EU internal security policy during the aftermath of the 2004 Madrid terrorist attack fell short of the expectations held by the leading EU Member States (Kaunert 2010; Bures 2011). Security policies and strategies which were formulated, arranged and performed by several governments were increasingly concentrated on detection, identification and ultimately, the deactivation of both immediate and potential threats in order to protect the public arena through the mechanisms of early warning, prevention and anticipation. These strategies were consistent with the nation-centric preventive approach defined by the 2004 Declaration on Combating Terrorism, the 2004 Hague Programme and the package of counterterrorist strategies adopted in late 2005 (with EU Counter-Terrorism strategy as a core).

Elements of the pre-crime approach were most clearly identified in the Strategy for Combating Radicalisation and Recruitment to Terrorism. Adopted as a separate document, it aimed to prevent individuals from turning to terrorism and to stop the next generation of terrorists from emerging. It proposed disrupting the recruitment activities of both individual and group actors for the purpose of terrorism, to engage in a dialogue with Muslim communities in order to promote moderate voices prevailing over extremist ones, and to promote security, justice and opportunity for all (Council of the EU 2005a, 1). With regard to the practical motives of emphasizing these preventative characteristics, the strategy utilized community policing and effective monitoring of the Internet, as well as people travelling to and within identified conflict zones. At the EU level, this strategy called for traditional goals, such as increased coordination of national policies, information sharing, as well as planning and exchanging good practices (Bossong 2008; Gruszczak 2008, Coolsaet 2010). Due to the conservative nature of the document, however, the methods and means defined in that document did not allow for a breakthrough in the general approach to terrorism and other risks to EU internal security.

Protracted and inconclusive work on new legislative proposals intended to strengthen cooperation in EU security policy eventually led to the fragmentation of prospective cooperation in home affairs. The G5 group established in 2003 by the five largest and most influential EU Member States - Germany, France, the UK, Italy and Spain - aspired to leadership in this field by providing a decision-making forum outside the framework of the EU. In May 2005, seven of the EU Member

States concluded the Prüm Treaty on the need to step up cross-border cooperation, particularly for the purpose of combating terrorism, as well as cross-border crime and illegal migration. The document envisaged a mutual exchange of information extracted from criminal records through the automated searching and comparison of DNA profiles, fingerprint data, vehicle registration data as well as information on terrorist subjects and illegal migration (Council of the EU 2005b; Balzacq et al. 2006; Bellanova 2008).

The spectre of a polycentric internal security governance for the EU, which would dilute its ultimate effectiveness, did not come to pass due to the policy shift of the leading EU member states towards a pro-Union stance regarding the prospects for a robust, efficient and firm strategy responding to the needs of policy planning and strategic guidelines in the field of internal security. The beginning of conceptual works on the next multiannual programme for the EU's area of freedom, security and justice and the establishment of a high-level advisory group on the future of European home affairs policy, (the so-called Future Group) allowed to orientate the dispersed views and perspectives towards coming imminent and inevitable challenges and tasks.

The Future Group's contribution to the debate on EU internal security was important, in particular because it stimulated a proactive approach and a much bolder attitude towards utilizing modern means and tools for the dual purposes of precaution and early warning. The Group recommended both closer cooperation between police and intelligence services in the Member States, and a guarantee of increased synergy between law enforcement agencies on a national level, possibly through networking and transnational workflow (Bizjak 2009). Furthermore, the Group suggested that EU agencies such as Europol and Eurojust, as well as the Joint Situation Centre (SitCen), should be strengthened and better positioned to serve Member States with regard to the exchange of intelligence (Future Group 2008a, 5; 2008b).

The Future Group was established in order to formulate a general approach towards a new vision of upcoming projects held in the subsequent multi-annual programme of developing the EU area of freedom, security and justice. This programme was prepared by the Swedish EU Presidency and subsequently adopted by the European Council in mid-December 2009, just after the entry into force of the Lisbon Treaty. *The Stockholm Program: An Open and Secure Europe Serving the Citizen* (European Council 2010) put a proper emphasis on prevention and control. Moreover, one can notice an evidently anticipatory approach.

> 'The best way to reduce the level of crime is to take effective measures to
> prevent them from ever occurring [emph. added], including promoting social
>   inclusion, by using a multidisciplinary approach which also includes
> taking administrative measures and promoting cooperation between
> administrative authorities, citizens of the Union that have similar

experiences and are affected in similar ways by crime and related insecurity in their everyday lives' (European Council 2010, 20).

In summary, while the prevention and deterrence of threats was important, disaster prevention through reducing the states' vulnerability to these events by developing a strategic approach, improving preparedness and increasing the effectiveness of potential responses were to be of equal value. These anticipatory elements reveal themselves in those parts of the document dedicated to the prevention of criminal acts. The Commission was tasked with assessing whether the networking of criminal records made it possible to prevent criminal offences from being committed; for example, through background checks to determine access to certain jobs, and whether it is possible to extend the exchange of information of these supervision measures (European Council 2010, 19).

The Stockholm Programme granted the necessary political authorization for a comprehensive strategic approach to internal security, which allowed for the enhancement of actions at the European level, combined with better coordination at the national level; the ambitions and intentions of EU institutions were to be reconciled with national sovereign interests (Brown 2011, 485-487). The European Council called upon the Council and the Commission to define an internal security strategy for the Union based on the principle of clarity regarding the specific division of tasks between the EU and the Member States. This includes stringent cooperation between Union agencies, which includes further improvement of information exchange, as well as the use of regional initiatives and cooperation schemes, and a horizontal approach in order to face complex crises and disasters (Buono 2009; Kaunert and Léonard 2010).

Nevertheless, the Stockholm Programme explicitly stated that a proactive approach is one of the basic elements of any future strategy for crime prevention. The Programme reflected on the necessity of a proactive and intelligence-led approach, as well as a focus on implementation and streamlining; the participants felt that preventative action deserved particular attention as an essential background for the eventual political declaration, which would signal a significant shift in the hitherto reactive EU internal security policy. Other provisions incorporated into the Programme regarding the adoption of this type of internal security strategy naturally met with an immediate reaction from the Spanish government, who were also preparing to take over the Council Presidency. Spain presented a draft of the new EU Internal Security Strategy (EUISS) already at the end of December 2009 in Madrid, and after having cleared intense scrutiny it was adopted by the EU Council in February 2010.

The changes to the existing strategies were to be extensive, as showcased in the following excerpt:

'Among the main objectives of the Internal Security Strategy for the EU are the prevention and anticipation of crime as well as of natural and man-made disasters, and the mitigation of their potential impact. Whilst effective prosecution of the perpetrators of a crime remains essential, a stronger focus on the prevention of criminal acts and terrorist attacks before they take place can help reduce the consequent human or psychological damage which is often irreparable. Our strategy must therefore emphasise prevention and anticipation, which is based on a proactive and intelligence-led approach as well as procuring the evidence required for prosecution' (Council of the EU 2010a, 11).

As a result of these changes, the arsenal of preventive, anticipatory and intelligence-based measures became quite impressive: analytical tools, early-warning systems, data pooling, systems of recording and transfer of sensitive data, risk analysis and capacity planning. According to the EUISS,

'This allows us to deepen our understanding of the different types of threats and their probability and to anticipate what might happen, so that we are not only prepared for the outcomes of future threats but also able to establish mechanisms to detect them and prevent their happening in the first place. For this reason, a comprehensive approach must be taken that is geared to constant detection and prevention of the threats and risks facing the EU in the various areas of internal security, and the main issues of concern to the public' (Council of the EU 2010a, 11).

The organisational framework regarding the enforcement of the principles, as well as the objectives of the EUISS, also appears to be innovative, at least to a certain extent. As a result, EU institutions and agencies that had already been reformed by the Lisbon Treaty and further strengthened on new legal grounds (especially in the case of Europol), obtained additional support on the part of the newly established Standing Committee on Internal Security (COSI).

As designed, the EUISS became a linchpin for a new model of internal security governance, one that is based on a more integrated approach tackling both the source and root causes of threats, risks and insecurity and not solely addressing the consequent effects and negative outcomes. In practical terms, the strategy's pre-crime objectives were met through a reinvigoration of the information exchange existing between law enforcement authorities in the Member States. This system also takes advantage of existing EU databases as well as improved operational cooperation between the EU's internal security agencies and bodies, such as Europol, Cepol, Eurojust and Frontex, and ensuring stringent coordination between them by the COSI.

In a follow-up of the EU Internal Security Strategy, the Belgian Presidency launched a project in 2011 which aimed to link the various national strategies of the Member States with political decisions at the EU level to create an effective way of operational activities between EU agencies and national law enforcement services. It crafted the *Harmony Project* in close cooperation with Europol, as well as the UK and the Netherlands, because of their experience in intelligence-led policing, so as to develop an integrated EU approach to crime prevention and combating terrorism through a comprehensive threat assessment and on this basis as an intelligence-led cooperation in action (Belgian Federal Police 2010).

The project envisioned linking all the requisite organizations within a horizontal approach, which would result in a better alignment between the activities of the EU agencies and combined with a vertical approach, meaning that the Member States could avail themselves of the opportunity to integrate EU tools and measures into their national strategies and policies. As a result, a genuine European policy cycle could be established on the grounds of the already existing EU instruments, policies and actions. In April 2010, a seminar was held in order to discuss the core concept and principles of a European policy cycle model. Those assembled at the seminar recognized that there was a need to further develop a coherent policy cycle on the basis of an intelligence-led policing approach. The Council at a meeting in Brussels on 8 and 9 November 2010 adopted conclusions on the creation and implementation of an EU-wide policy cycle for organised and serious international crime on the basis of a new 'intelligence product': the European Union Serious and Organised Crime Threat Assessment (Council of the EU 2010b) .

Next years have shown, however, that the initial impetus for a comprehensive internal security governance in the EU was lost. Likewise, the pre-crime approach has been limited to certain elements of policy cycle, most of all criminal intelligence, risk analysis and threat assessments. These issues are elaborated in the remainder of this paper.

EU Criminal Intelligence Model

EU security policy has acquired a multidimensional character in the past decade, due to new forms of emerging threats and challenges as well as varied types of response. The levels of EU security policy differed in many respects, subject to issues, areas, methods, tools and policies applied to cope with detected or identified problems. Approaches worked out for the effective operation in particular fields of security were aiming to tackle any single issue in a specific manner, giving thus opportunity for EU institutions and agencies to intervene in political, economic, diplomatic, or even military way. Before 9/11, however, EU

justice and home affairs cooperation, despite its reinforcement as a result of the 1999 Amsterdam reform of EU treaty law, was relatively loose and dependent on Member States' particular interests or national determinants. Intergovernmental arrangements and EU secondary legal instruments constituted a general framework for internal security policy yet left inside a vast area of variegated activities by Member States focused on narrowly defined national interests and local perception of security problems and challenges.

The events of 9/11 highlighted the critical importance of intelligence for effective prevention and combating of terrorism and transnational crime. However, it did not have any special impact on the capabilities of EU legal and institutional arrangements to establish a genuine intelligence-led policing model. Some attempts at intensifying and enlarging the scope of intelligence cooperation at EU level, due to the lack of unanimity and the deficit of trust among the Member States, did not yield the expected results (Bures 2006, 62-63; Müler-Wille 2006; Duke 2006, 619-620).

This picture altered in the immediate aftermaths of the 11 March 2004 terrorist attack in Madrid. The EU's institutions placed particular emphasis on the exchange of information and intelligence between law enforcement authorities of the 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 Council in the Hague Programme of November 2004 set the goal of 'setting up and implementing a methodology for intelligence-led law enforcement at EU level.' (European Council 2004, 9). A British proposal submitted to Interior Ministers gathered at an informal meeting in September 2005 contained what may have been considered the 'missing link' in the creation of a potential EU intelligence tradecraft. A consultation paper delivered by the UK Home Office introduced the idea of a European Criminal Intelligence Model (ECIM) based on the principles of intelligence-led policing and evidently inspired by the UK's National Intelligence Model (UK Presidency 2005, 1). According to the UK Presidency, an ECIM should benefit EU Member States by:

- improving knowledge of serious and organised crime through more effective collection, exchange, and analysis of information;

- increasing the effectiveness of Europol and other relevant EU bodies;

- achieving better operational results;

- allowing all Member States as well as EU institutions to observe a common methodology for tackling serious and organised crime in the EU (UK Presidency 2005, 1).

The ECIM was marked by a 'shift from reactive policing to a problem solving approach, based on analysis, by developing action plans (focused on crime prevention as well as on repressive action) and involving multiple actors (both private and public partners)' (Council of the EU 2010c, 8). According to Brady, 'the ECIM sets out how the EU can achieve this by ensuring national police forces, Europol's criminal intelligence analysts and the police chiefs' operations work together against the same criminal threats' (Brady 2008, 106). Intelligence-led policing principles which were the critical underpinning for the ECIM, were based on the assumption that EU agencies and institutions in strict cooperation with the Member States must first improve its knowledge of various aspects of cross-border and international criminality, while also developing an intelligence cycle leading to strengthened and accurate operational capabilities (Nunzi 2007, 148).

Europol was pointed as the 'central EU capability to receive, store and analyse this collected information' and to support operational activities of the Member States based on Europol's earlier strategic assessments. However, the eventual application of the ECIM was predetermined by Europol's capabilities, which had been reduced by legal provisions and organisational schemes, as well as the inability of the Member States to exercise a joint will or exhibit an openness for advanced cooperation in the exchange of information and intelligence in the area of transnational criminal justice. The Hague Programme formulated a prospective solution to the challenge of granting mutual access to criminal intelligence data stored in the individual databases of the Member States, based on the principle of availability, but it collapsed in the face of the inherent bureaucratic inflexibility within the decision-making process at the EU level. 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, it neither significantly improved the efficiency of information exchange system in the EU, nor did it contribute to the feasibility of the ECIM. Furthermore, the availability of police data and intelligence was subject to numerous regulations, rules and working arrangements set on national, legal and political grounds (Bigo 2006; Elsen 2007). Given the clear lack of confidence among law enforcement agencies, and the constant deficit of trust for Europol and Eurojust, in the end flexible and efficient prevention was hardly viable at the EU level. Instead, it followed other intergovernmental channels and arrangements, both formal and informal (Gruszczak 2009, 93-94).

Europol, on the basis of the new Decision adopted in April 2009, was endowed with enhanced capabilities in the area of information management, intelligence production and sharing, as well as operational support for the Member States. Europol's strategy for the period 2010-2014 assigned this entity the role of EU criminal information hub and the centre for law enforcement expertise. Europol should also support law enforcement operations in the Member States,

mostly through the delivery of analysis and intelligence. Europol was also tasked to lead the further development of the ECIM. In this regard, it should develop a common EU approach for targeted collection and sharing of key criminal information, integrated analysis of financial intelligence linked to all crime phenomena, identification of top criminal targets. It should also improve and strengthen the OCTA methodology and promote ECIM principles among national authorities in the Member States as well as EU institutions and agencies (Europol 2009).

The European Criminal Intelligence Model is based on the assumption that the tasking and co-ordination processes at EU level should be fully dependent on the key intelligence products conceived as the 'deliverables' by which intelligence-led policing can be implemented. These key intelligence products included strategic assessments, tactical assessments, risk analyses and problem profiles. All intelligence work should be supported by the knowledge products and system products as elements that provide quality assurance to the ECIM. In this regard, the functioning of international co-operation and liaison arrangements, including Europol, was meant to provide support for analysis of terrorism and organised crime.

Risk Analysis Model

Risk analysis is a widely used tool to understand problems and identify challenges and hazards in many areas of contemporary life, especially under conditions of uncertainty (Frenkel, Hommel and Rudolf 2005; Jablonowski 2006; Power 2007; Vellani 2007; Yoe 2012). With respect to security, risk assessment is one of the foundational skills developed by analysts, experts and decision-makers because it estimates the probabilities of exposure to certain threats and hazards, helps to anticipate problems before they result in an irreversible breakdown and is a basis for appropriate countermeasure options (Löfstedt 2005; Jablonowski 2006; Norman 2010).

EU internal security governance has been progressively determined by skills, measures and technologies employed to estimate the identified sources and types of risk, assess the probability of its appearance and work out appropriate solutions at EU level. While criminal intelligence focused on serious threats generated by domestic and transnational organized groups, risk analysis is more oriented to "soft" threats, which do not bring about an explosive situation undermining the foundations of public order, rule of law or state authority but may produce long-term negative consequences for systemic stability, public accountability and reliability of state institutions. One can say that criminal intelligence addresses the problem of legal order while risk analysis is referred to societal trust and

legitimacy of state authority. Generally, risk analysis responds to certain needs of EU institutions and agencies with respect to ideological, legal, human and systemic prerequisites of freedom, security and justice in the European Union. Most of all, risk analysis serves to identify "precautionary regions", or "danger zones" (Jablonowski 2006, 42-43), reduce uncertainty and contribute to effective solutions adopted by EU institutions or agencies.

For decades, migration has exerted a huge impact on European societies, economies and – last but not least - identity. According to Eurostat, as of 1 January 2012 there were 33 million foreigners living in the EU (6.5 per cent of the total population). Of these, 20.7 million are citizens of non-EU countries (Eurostat 2013). The illegal foreign resident population in the EU is estimated at 1.9 to 3.8 million in 2008. Some sources claim the number of irregular migrants is 2.8-6 million or even up to 8 million (CLANDESTINO 2009). Over half of illegal immigrants entered the EU legally but became illegal due to overstay (European Commission 2008, 2-3). In 2010 540,000 illegal immigrants were apprehended in the EU but only 226 000 (around 40 per cent) of these were effectively removed (European Commission 2011, 4). The European Union, with 500 million inhabitants, over 42,000 km of coastline, almost 9,000 km of land borders and approximately 1800 border crossing points sees every year around 700 million external border crossings. About a third of these border crossings are made by third country nationals who are checked at the crossing points at EU external borders.

Obviously enough, EU external borderlands have been one of the most sensitive "precautionary areas" for EU Member States and its citizens for they were highly exposed to illegal migration and unfounded asylum seeking. The fear of increasing migratory pressure and accumulation of asylum application underpinned the development of immigration and asylum legal inventory as well as the building up of an integrated border management system aiming to reinforce the EU's "external shield" and reduce probability of risk-prone transfers of persons and goods into the territory of the Member States. One of the elements of exclusionary approach to immigration and asylum was the establishment of Frontex – an EU agency for the management of operational cooperation at EU external borders. According to Council Regulation (EC) No 2007/2004 establishing Frontex, amended in October 2011 (Council of the EU 2004; Council of the EU 2011), this agency facilitates and renders more effective the application of existing and future Union measures relating to the management of external borders. The tasks enumerated in the above mentioned documents include the carrying out of risk analyses, including the assessment of the capacity of Member States to face threats and pressure at the external borders, and the participation in the development of research relevant for the control and surveillance of external borders. As regards information exchange and intelligence analysis, Frontex is responsible for developing and operating information systems that enable swift and reliable exchanges of information regarding emerging risks at the external borders, as well

as providing the necessary assistance to the development and operation of a European border surveillance system and, as appropriate, to the development of a common information sharing environment, including interoperability of systems. More specifically, the agency is assigned to develop and apply a common integrated risk analysis model. It prepares both general and tailored risk analyses to be submitted to the Council and the Commission. Article 4 of the Council Regulation No 2007/2004 stipulates that: 'For the purpose of risk analysis, the Agency may assess, after prior consultation with the Member State(s) concerned, their capacity to face upcoming challenges, including present and future threats and pressures at the external borders of the European Union, especially for those Member States facing specific and disproportionate pressures. To that end, the Agency may assess the equipment and the resources of the Member States regarding border control. The assessment shall be based on information given by the Member States concerned, and on the reports and results of joint operations, pilot projects, rapid interventions and other activities of the Agency' (Council of the EU 2004).

Given the handful of migration statistical data mentioned above, depicting intensity of migratory movements in the EU, the problem of acquiring, processing, evaluating and analysing relevant information for intelligence purposes seems to be very demanding. Frontex and EU Member States have intended to work out a comprehensive solution consisting in the integration of various forms of intelligence and risk analysis through interconnected information sources and datasets dedicated to the constant or emerging security-related issues. Frontex has been granted with certain competences regarding information management. It collates data mainly from Member States, which are obliged to provide the Agency with all necessary information regarding the situation and possible threats at the external borders. In addition, EU bodies as well as public media and other open sources of information are taken into consideration. Most importantly, the amended Frontex regulation authorises the agency to collect and process personal data of individuals who are subject to operational activities conducted or commanded by Frontex, like joint return operations, pilot projects and rapid interventions at the external borders, in order to contribute to the security of the Member States. Collated information, including personal data, is further processed for strategic and operational purposes as well as a contribution to the analytical and operational work of other EU law enforcement agencies, mainly Europol.

Risk analysis is the core part of Frontex's intelligence tradecraft. It fits the logic of analysis cycle, being the starting point of all Frontex operational activities as well as delivering a picture of the situation at the EU's external borders, contributing to training purposes and responding to the needs of principal customers: EU agencies and Member States.

A framework for risk analysis was created in 2003 and consequently developed after the establishment of the Frontex agency. It is called CIRAM - the

Common Integrated Risk Analysis Model. It was implemented by the Risk Analysis Centre set up in 2003 by EU Member States and served as a tool of strategic intelligence used by the Strategic Committee on Immigration, Frontiers and Asylum (SCIFA) serving the JHA Council of the EU. CIRAM was based on a six-field matrix, bringing together elements of criminal intelligence and risk assessment (Carrera 2007, 15-16). CIRAM was updated in 2011 in order to better respond to the changing external environment of the EU, to deal effectively with new types of risks and threats and to reflect the legal changes, especially the new Schengen Borders Code and the Frontex Regulation, both of which emphasised risk analysis as a key tool in ensuring the optimal allocation of resources and efficiency of equipment (Frontex 2013a, 11).

Currently CIRAM is characterised by a management approach to risk analysis that defines risk as a function of the threat, vulnerability and impact (Frontex 2013a, 11). It is utilised for strategic and operational purposes. Concerning the latter, it supports the coordination of joint operations at the external borders conducted or coordinated by Frontex. It provides a background for an overall assessment of conditions, determinants and circumstances existing in the area of a planned joint operation at EU external borders. This picture is a sort of security landscape and is drawn on the basis of vast data flow containing various detailed information delivered by operational personnel made available by the Member States as well as acquired from public sources. This type of analysis is focused on identifying areas and sources of elevated risk or imminent threats and deciphering migratory routes, the main nationalities or countries of origin of migrants as well as modi operandi of criminal groups or smuggling networks operating in the area of Frontex's planned activities.

Operational analytical products are evidently based on a pro-active assessment of security environment, including anticipation of threats and hazards and early warning. Knowledge management and risk analysis are methods serving to build up preparedness and resilience to endemic problems and security challenges existing at the external borders. They also underpin strategic analysis, wherein CIRAM is orientated to the needs of decision-makers in the Member States, officials in EU institutions and agencies, border authorities and international organisations. To be effective and reliable in its analytical properties, CIRAM relies on a four-tier access control model that involves gathering information from numerous sources dispersed over the territory of EU member states. To this end, the Frontex Risk Analysis Network (FRAN) was established in 2007. It provides the framework for sharing knowledge and producing analytical and strategic reports on the current state of play at the external borders linking the intelligence networks of individual countries with Frontex (Frontex 2013b). The cooperative framework of the FRAN and its subsidiary, the European Union Document-Fraud Risk Analysis Network (EDF-RAN), feeds Frontex Risk Analysis Unit (RAU) with data which are processed, analysed and disseminated in form of analytical products. The most important are

quarterlies, semi-annual and annual risk analyses. Moreover, RAU issues occasional documents and other tailored risk-analysis products.

Risk analysis model implemented by Frontex reflects pro-active approach to public order and internal security of the EU. Pre-crime perspective addresses not only 'crimes of arrival', i.e. inflow of irregular migrants seeking refugee status. It is mostly dealing with the problem of increasing criminality at EU external borders, taking form of transnational organized criminal networks involved in trafficking in human beings. This is why Frontex's methodology combines quantitative risk analysis, which relies on mathematical models and techniques to identify, quantify and manage exposures, with qualitative risk management, which focuses primarily on experience, judgment and common sense. However, the prevalence of quantitative data in Frontex's analytical tradecraft suggests that the agency is focused on 'hard' border security issues that could underpin cost-benefit approach to EU immigration and asylum policies. This means that the horizon on an emerging security landscape is a part of 'borderwork' consisting in the performance of specific power relations seeking to produce and reproduce a bounded identity of 'aliens' (Hooper 2004, 218; Vaughan-Williams 2008). In this respect, selective differentiation at the external borders seeks to facilitate information management and enhance risk analysis capabilities of Frontex as well as national risk assessment units in the Member States.

Threat Assessment Methodology

Risk analysis and threat assessment are an integral part of the policy cycle since they address the security requirements of the European Union in terms of integrity, availability, accountability and confidentiality. Following Vidalis (2003, 5) we conceive a threat assessment as a statement of threats that are related to vulnerabilities of a given entity and to threat agents (hostile states, terrorist groups, criminal organizations, irregular migrants), and also a statement of the believed capabilities that those threat agents possess. Threat assessment is more of qualitative nature. It takes into account numerous categories of data delivered by authorized stakeholders or extracted from open sources.

The development of an integrated threat assessment model in the EU was restricted by the low level of mutual cooperation in policing and criminal justice, differences in national perspectives on security threats and the lack of large-scale IT systems enabling secure information exchange.

As we mentioned above, in 2005 a European Criminal Intelligence Model was proposed by the UK. One of its elements was the improvement of knowledge of serious and organised crime through more effective collection, exchange, and

analysis of information. In parallel, the UK Presidency also submitted to the Council draft conclusions on intelligence-led policing and the development of the Organised Crime Threat Assessment (OCTA) (Council of the EU 2005c). It was stipulated that Europol would be in charge of producing an OCTA in close cooperation with Member States obliged to facilitate and instigate the transmission of structured information and intelligence in accordance with intelligence requirements prepared by Europol and issued through the Heads of Europol National Units. Europol would also communicate that intelligence requirements to EU agencies and bodies and to third countries and organisations with which it had co-operation agreements. The information and criminal intelligence obtained from the above listed entities should be used to produce the OCTA.

In 2006, the first Organized Crime Threat Assessment was published by Europol, replacing the Organized Crime Report prepared annually since 1993. The then-Director of Europol, Max-Peter Ratzel, described OCTA as 'a core product of the intelligence-led policing concept' (Europol 2006, 3). It was pointed out in the report that 'The OCTA, being a forward-looking document, will help decisionmakers identify strategic priority areas in the fight against serious and organised crime and to initiate an intelligence process to define operational targets. By doing so, the OCTA will also support the streamlining of law enforcement activities at a European and regional level.' (Europol 2006, 4). Intelligence tradecraft employed in the OCTA was described in scarce words: 'The OCTA is based on a multi-source approach, including law enforcement and non-law enforcement sources. These sources include various European agencies as well as the private sector. A specific emphasis is put on elaborating the benefits of an intensified public-private partnership.' (Europol 2006, 4). Methodology was Achilles' heel of those yearly reports and raised criticism on the part of experts and practitioners (van Duyne 2007; Zoutendijk 2010). It rose up during the discussion on the reinforcement of preventive aspects of EU internal security policy and particularly after the adoption of the Internal Security Strategy highlighting prevention, anticipation and intelligence-led approach.

In a follow-up of the EU Internal Security Strategy, a seminar was held in April 2010 in order to discuss the core concept and principles of a European policy cycle model. Those assembled at the seminar recognised that there was a need to further develop a coherent policy cycle on the basis of an intelligence-led policing approach. The Council at a meeting in Brussels in November 2010 adopted conclusions on the creation and implementation of an EU-wide policy cycle for organised and serious international crime on the basis of a new 'intelligence product': the European Union Serious and Organised Crime Threat Assessment (EU SOCTA) (Council of the EU 2010b).

The Serious and Organised Crime Threat Assessment Methodology was validated by COSI at its meeting on 25 June 2012 (Council of the EU 2012). It was

implemented for the first time in the 2013 organised crime threat assessment published by Europol in March 2013 (Europol 2013). The SOCTA constitutes the core part of the EU policy cycle and is deemed necessary for an effective implementation of the intelligence-led approach ensuring that the most relevant threats are properly addressed and that analytical products developed and launched by appropriate EU agencies directly feed political decision-making in the EU. As a result, the methodological work on the new threat assessment in general was following the typical intelligence cycle, focusing both on delivery capabilities of major contributors (i.e. Europol and member states' law enforcement services) as well as the previously agreed customer requirements. The fundamental feature of the SOCTA is its anticipating perspective on transnational organised criminality. It was stressed in the SOCTA methodology, that 'The SOCTA is a present- and future-oriented threat assessment. It goes a step further then a situation report (which is retrospective and mainly statistical) as it takes into account possible future developments.' (Council of the EU 2012, 4). Hence, the SOCTA methodology includes a 'watch list' of probable threats that need to be monitored as well as 'horizon scanning' to detect and analyse new and emerging threats from serious and organised crime.

The conceptual model, worked out by Europol in cooperation with the SOCTA expert group (composed of EU Member States, Europol's third partner countries and organisations, European Commission and Council General Secretariat), consists of the four steps: the focus, the tools, the analysis and assessment, and the results. It begins with three focus points: organised criminal groups, serious and organised crime areas, and the environment on which they have an effect and by which they are facilitated. These elements are assessed with the use of three types of indicators and additionally Crime Relevant Factors. The latter are facilitating factors and vulnerabilities in the environment that have an influence on current and future opportunities or barriers for organised criminal groups and crime areas. These factors are analysed via horizon scanning, which aims to identify future trends in society and future crime threats making use of a Delphi exercise.

The analysis and assessment reflects the very structure and organisation of Europol and police cooperation network centred on this agency. The analytical work starts from the reaching into the resources held by Europol which are catalogued and stored in Analytical Work Files. They may be combined with threat notices on new and emerging trends, specific threat assessments and other strategic reports developed at Europol. Additionally open sources intelligence is used to scan the crime environment. A preliminary analysis contributes to the development of tailored EU intelligence requirements. Similarly to the 'old' OCTA, intelligence requirements are contained in questionnaires sent to Member States as well as non-EU states and organisations that have strategic or operational agreements with Europol.

The core part of the analysis process is the processing of the data received from stakeholders and acquired from open sources and the assessment of the indicators and crime relevant factors. Adopting a holistic approach, Europol aims at interconnecting the available data sets and detecting synergies between threat assessment and horizon scanning as well as current and future threats. As a result, a list of recommended priorities on organised criminal groups and areas are formulated and delivered to the customers. These priorities, accompanied by argument maps, should be particularly useful in the preparation of multi-annual strategic plans in a later phase of the policy cycle (Council of the EU 2012).

Comparing SOCTA to its predecessors, in the perspective of pre-crime anticipatory approach, it seems that the new criminal intelligence product offered by Europol is much more advanced, rich and substantial. First of all, tradecraft employed in SOCTA analysis cycle is more developed and evidently highlights potential future trends and issues (Europol 2013). It is mining a considerable amount of information and data acquired from variegated sources and bases. Next, it introduces to Europol's analytical practice methods, tools and techniques typical for criminal intelligence models implemented by leading countries, not only in Europe, but also in the other continents. This methodological upgrade should bring about a prospective modernization of tradecraft in EU criminal intelligence area. Finally, threat assessment methodology embedded in SOCTA seems to be a good benchmark, or even best practice, for Member States which lag behind the leading countries in what concerns intelligence capabilities and information management. So, EU criminal intelligence tradecraft may encourage them to a more intense and productive cooperation with Europol in the exchange of information and criminal data.

Academic advisors to the SOCTA analytical team in Europol aptly grasped the value added by SOCTA to pre-crime approach to EU internal security: 'The SOCTA analysis brings to the foreground the dilemma and problems of prediction (that is often necessarily actuarial in character and therefore backward looking), contrasted with the need to be forward looking going beyond historical data to extrapolate to identify future change, and to facilitate effective proactive operational responses. A way of mitigating the difficulty of this may be the development at the Europol level of continuous crime trend scanning, extending the SOCTA process to support a more proactive approach.' (Europol 2013, 44).

SOCTA is a great step forward in the development and enrichment of EU criminal intelligence tradecraft. It does not mean, however, that this product perfectly fits the pre-crime anticipatory approach to internal security of the Union. The methodology is still behind the state-of-the-art applications employed by global powers. The final product still depends much on the contributions and uploads from Member States. Given the variety of 'rules of engagement' applied by national law enforcement services and thus responses to intelligence requirements

formulated by Europol, intelligence analysis made by this agency often falls short of expectations of practitioners, especially national intelligence officials in Member States. Following SOCTA methodology, crime matrices and cognitive maps could be created although so far, referring to the first ever SOCTA report published in 2013, one cannot find hard evidence of such advanced pro-active approach on the part of Europol. Nonetheless, SOCTA proves the qualitative potential of Europol and its ability to take advantage of diversified elements of criminal intelligence tradecraft.

Conclusions

Didier Bigo noted that, 'Pre crime strategy is then the child of intelligence led policing and the amplification of the tendency to have a *proactive* attitude towards crime and to try to control crime by analysing its patterns, its location, its occurrences and situations' (Bigo 2012). It seems that the observation made by the eminent French scholar is shared by Member States and EU institutions and agencies responsible for the proper EU internal security governance. Strategic guidelines, political decisions and legal instruments adopted at EU level clearly determine the future of cooperation in the field of policing and criminal justice in the Union. As the present author already noticed, the centre of gravity in the area of intelligence co-operation among EU Member States has been concentrated rather on direct collaboration among the national services, quite often outside the framework of the EU (Müller-Wille 2008, 55-58). The logic of European cooperation inclined to search for a 'missing link' in EU security policies and strategies – that of intelligence. Intelligence-led policing and criminal information management were considered to be a novel approach, taking advantage of communication technologies, large-scale EU-wide IT systems, forensic computer programmes and enhanced analytical capacities. Ongoing debate on an intelligence-led policing model and its practical benefits has led its participants towards the strategic thinking underlining the importance of linkages between national intelligence models, and international approaches to criminal threats and terrorist menace. The challenges of security governance, risk management, policy implementation and anticipatory decision-making were noticed also in the field of law enforcement. This explains the decision to launch an ECIM, to develop or amend its certain elements (policy cycle, threat assessments, information management) and – most importantly – take it as a relevant practical tool in the realm of counterterrorism and criminal prevention in the EU (Gruszczak 2013, 34-36).

In order to succeed, the pre-crime approach requires credible intelligence that is subjected to effective policing within local circumstances, crime hotspots and areas of elevated risk. As a result, criminal databases are rapidly inflating,

containing information stored automatically or condensed into analysis files, and reprocessed as needed for certain operational and cognitive purposes. The Intelligence-led policing, criminal intelligence models and policy cycles are evidence of efforts undertaken by competent EU institutions and agencies, in response to stimuli coming from particular Member States, in order to improve the management of sensitive information and criminal data delivered by the Member States.

Intelligence process is still decentralised and subject to national predilections and habits, or national security cultures, which quite often restrict the scope of involvement in intelligence cooperation at EU level. The implementation of EU policy cycle for organised and serious international crime has been an important event because for the first time a common single framework for criminal intelligence tradecraft was established to stimulate both Member States and EU agencies and institutions to enhance their capacity to deliver valuable inputs and obtain valuable and useful outcomes. This is crucial regarding prospects for the emergence of a robust, effective and legitimate intelligence community in the EU. So far, intelligence products offered by EU agencies are fairly useful but they lack high credibility due to restrictions imposed by individual Member States on the transmission of sensitive information and raw material they possess. This may result from the low confidence in EU-led methods, instruments and measures adopted in the realm of criminal intelligence. But such a sceptical attitude do not necessarily corresponds with the real capabilities of EU agencies.

Besides the leading products like Europol's SOCTA and TE-SAT or Frontex's FRAN and ARA, one can find numerous tailored analyses addressing specific requests by consumers, especially responding to the needs concerning prevention, anticipation and foreknowledge about the most serious threats, risks and hazards. These products seek to satisfy the strategic and operational needs of law enforcement services in Member States and they also attempt to develop and widen cognitive capabilities of an EU intelligence community emerging on grounds of internal security governance.

Intelligence tradecraft developed in recent years in the field of EU internal security has been characterised by the progressive adaptation and implementation of qualitative and quantitative methods of data analysis and information management by competent EU agencies, most of all Europol and Frontex. This trend corresponds with the reinforcement of the pre-crime approach focused on anticipation, early detection and warning of potential and substantial threats and hazards. Strategic intelligence is the area where the EU can and should convince its Member States and external partners of its utility, relevance and appropriateness. A continuously improved intelligence tradecraft is an argument for the further development and enhancement of the pre-crime approach to EU internal security governance.

References

Ackerman, Bruce (2006) *Before the next attack: preserving civil liberties in an age of terrorism* (New Haven, CT and London: Yale University Press)

Adey, Peter and Ben Anderson (2012) 'Anticipating emergencies: Technologies of preparedness and the matter of security', *Security Dialogue* 43, 99-117

Agrell, Wilhelm (2002) When everything is intelligence – nothing is intelligence, The Sherman Kent Center for Intelligence Analysis Occasional Papers, 1, <https://www.cia.gov/library/kent-center-occasional-papers/vol1no4.htm>
Amoore Louise and Marieke de Goede (2008) 'Transactions after 9/11: the banal face of the preemptive strike', *Transactions of The Institute of British Geographers* 33, 173–85

Anderson, Ben (2010a) 'Security and the future: Anticipating the event of terror', *Geoforum* 41, 227-235

Anderson, Ben (2010b) 'Preemption, precaution, preparedness: Anticipatory action and future geographies', *Progress in Human Geography* 34, 777–798

Anderson, Malcolm and Joanna Apap (2002) *Striking a Balance between Freedom, Security and Justice in an Enlarged European Union* (Brussels: Centre for European Policy Studies)

Aradau, Claudia (2008) 'Forget Equality? Security and Liberty in the 'War on Terror', *Alternatives: Global, Local, Political* 33, 293–314

Aradau, Claudia and Rens van Munster (eds) (2011) *Politics of Catastrophe: Genealogies of the Unknown* (London and New York: Routledge)

Aradau, Claudia and Rens van Munster (2012) The Time/Space of Preparedness: Anticipating the "Next Terrorist Attack"', *Space and Culture* 15, 98-109

Argomaniz, Javier (2011) *The EU and Counter-Terrorism. Politics, polity and policies after 9/11* (London and New York: Routledge)

Balzacq, Thierry, Didier Bigo, Sergio Carrera and Elspeth Guild (2006) 'The Treaty of Prüm and EC Treaty: Two Competing Models for EU Internal Security' in Thierry Balzacq and Sergio Carrera (eds) *Security Versus Freedom? A Challenge for Europe's Future* (Aldershot and Burlington: Ashgate), 35-44

Balzacq Thierry and Sergio Carrera (eds) (2006) *Security Versus Freedom? A Challenge for Europe's Future* (Aldershot and Burlington: Ashgate)

Bellanova, Rocco (2008) 'The "Prüm Process:" The Way Forward for EU Police Cooperation and Data Exchange?' in Elspeth Guild and Florian Geyer (eds) *Security versus Justice? Police and Judicial Cooperation in the European Union* (Aldershot and Burlington: Ashgate), 203-221

Berman, Paul (2004) *Terror and Liberalism* (New York and London: W.W. Norton & Company)

Bigo, Didier (2006) 'Liberty, whose Liberty? The Hague Programme and the Conception of Freedom' in Thierry Balzacq and Sergio Carrera (eds) *Security Versus Freedom? A Challenge for Europe's Future* (Aldershot and Burlington: Ashgate), 35-44

Bigo, Didier (2012) 'The future perfect of (in)security (P8) : Pre-crime strategy, Proactivity, Preemption, Prevention, Precaution, Profiling, Prediction, & Privacy' < http://www.interdisciplines.org/paper.php?paperID=342>

Bigo, Didier and Anastassia Tsoukala (eds) (2008) *Terror, Insecurity and Liberty. Illiberal practices of liberal regimes after 9/11* (Abingdon and New York: Routledge)

Bizjak, Ivan (2009) 'The reports presented by the "Future Groups" and their proposed solutions for the future of EU criminal justice', *ERA Forum* 10, 343-354

Blinken, Antony J (2003–04) 'From Preemption to Engagement', *Survival* 45, 33-60

Bohm, Nicholas and Stephen Mason (2010) 'Identity and its verification', *Computer Law & Security Review* 26, 43–51

Bobbitt, Philip (2008) *Terror and Consent. The Wars for the Twenty-First Century* (New York: Alfred A. Knopf)

Bossong, Raphael (2008) 'The Action Plan on Combating Terrorism: A Flawed Instrument of EU Security Governance', *Journal of Common Market Studies* 46, 27-48

Botterhuis, Lineke, Patrick van der Duin, Paul de Ruijter and Peter van Wijck (2010) 'Monitoring the future. Building an early warning system for the Dutch Ministry of Justice', *Futures* 42, 454–465

Brady, Hugo (2008) 'Europol and the European Criminal Intelligence Model: A Non-state Response to Organized Crime', *Policing* 2, 103–109

Brown, David (2011) 'The Stockholm solution? Papering over the cracks within the area of freedom, security and justice', *European Security* 20, 481-503

Buono, Laviero (2009) 'From Tampere to The Hague and beyond: towards the Stockholm Programme in the area of freedom, security and justice', *ERA Forum* 10, 333-342

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

Bures, Oldrich (2011) *EU Counterterrorism Policy: A Paper Tiger?* (Farnham and Burlington: Ashgate)

Bzostek, Rachel (2008) *Why not preempt? : security, law, norms and anticipatory military activities* (Aldershot and Burlington, VT: Ashgate)

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

Carroll-Mayer, Moira, Ben Fairweather and Bernd Carsten Stahl (2008) CCTV Identity Management and Implications for Criminal Justice: some considerations', *Surveillance & Society* 5, 33-50

CLANDESTINO (2009) Size and Development of Irregular Migration to the EU. CLANDESTINO Research Project, <http://irregular-migration.net/typo3_upload/groups/31/4.Background_Information/4.2.Policy_Brief s_EN/ComparativePolicyBrief_SizeOfIrregularMigration_Clandestino_Nov09_2.pdf>

Coolsaet, Rik (2010) 'EU counterterrorism strategy: value added or chimera?', *International Affairs* 86, 857-873

Cooper, Melinda (2006) 'Pre-empting emergence' *Theory, Culture & Society* 23, 113–135

Council of the EU (2004) 'Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union', *Official Journal of the European Union* L 349, 25 November

Council of the EU (2005a) 'The European Union Strategy for Combating Radicalisation and Recruitment to Terrorism', doc. 14781/1/05 REV 1 LIMITE, Brussels, 24 November

Council of the EU (2005b) 'Prüm Convention', doc. 10900/05 LIMITE, Brussels, 7 July

Council of the EU (2005c) 'Council conclusions on intelligence-led policing and the development of the Organised Crime Threat Assessment (OCTA)', doc. 10180/4/05 REV 4 LIMITE, Brussels, 3 October

Council of the EU (2010a) 'Draft Internal Security Strategy for the European Union: "Towards a European Security Model"', doc. 5842/2/10 REV 2, Brussels, 23 February

Council of the EU (2010b) 'EU Policy Cycle', doc. 12657/1/10 REV 1 LIMITE, Brussels, 3 September

Council of the EU (2010c) 'Result of the "Harmony" project - "A generic European Crime Intelligence Model - Bringing together the existing instruments and strengthening Europol's central role', doc. 14851/10, Brussels, 25 October

Council of the EU (2011) 'Regulation (EU) No 1168/2011 of the European Parliament and of the Council of 25 October 2011 amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union', *Official Journal of the European Union* L 304, 22 November

Council of the EU (2012) 'Serious and Organised Crime Threat Assessment (SOCTA) – Methodology', doc. 12159/12, Brussels, July 4

Daalder, Ivo H (ed) (2007) *Beyond Preemption. Force and Legitimacy in a Changing World* (Washington, DC: Brookings Institution Press)

Deflem, Mathieu (2010) *The policing of terrorism: organizational and global perspectives* (Abingdon and New York: Routledge)

De Goede, Marieke (2008) 'The Politics of Preemption and the War on Terror in Europe', *European Journal of International Relations* 14, 161-85

De Goede, Marieke (2011) 'European Security Culture. Preemption and Precaution in European Security', Inaugural lecture delivered upon accession to the office of hoogleraar Politicologie at the University of Amsterdam on 27 May 2011 (Amsterdam: Vossiuspers UvA)

DeLeo, Rob A. (2010) 'Anticipatory–Conjectural Policy Problems: A Case Study of Avian Influenza', *Risk, Hazards & Crisis in Public Policy* 1, 147-184

Duke, Simon (2006) 'Intelligence, security and information flows in CFSP', *Intelligence and National Security* 21, 604-630

Elsen, Charles (2007) 'From Maastricht to The Hague: the politics of judicial and police cooperation', *ERA Forum* 8, 13-26

Ericson, Richard V (2007) *Crime in an Insecure World* (Cambridge and Malden: Polity Press)

European Commission (2008) 'Commission Staff Working Document accompanying document to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Preparing the Next Steps in Border Management in the European Union. Summary of the Impact Assessment', doc. SEC(2008) 154, 13 February

European Commission (2011) 'Communication from the Commission to the European Parliament and the Council - Smart borders - options and the way ahead', doc. COM(2011) 680 final, Brussels, 25 October

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, 4 May

Europol (2006) *EU Organised Crime Threat Assessment 2006* (The Hague: Europol)

Europol (2009) 'Europol Strategy 2010 – 2014', EUROPOL Management Board, doc. 1424-73r1, 2 November

Europol (2013) *SOCTA 2013. EU Serious and Organised Crime Threat Assessment* (The Hague: European Police Office)

Eurostat (2013) Migration and migrant population statistics, <http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Migration_and_migrant_population_statistics#Foreign_and_foreign-born_population>

Feinstein Lee and Anne-Marie Slaughter (2004) 'A Duty to Prevent', *Foreign Affairs* 83, 136–50

Fitzgibbon, Wendy (2004) *Pre-emptive criminalisation: risk control and alternative futures* (London: NAPO ICCJ Monograph)

Frenkel, Michael, Ulrich Hommel and Markus Rudolf (eds) (2005) *Risk Management. Challenge and Opportunity* (Berlin and Heidelberg: Springer) 2nd ed

Friedrichs, Jörg (2008) *Fighting Terrorism and Drugs. Europe and international police cooperation* (London and New York: Routledge)

Frontex (2013a) 'Annual Risk Analysis 2013' (Warsaw: Frontex Risk Analysis Unit)

Frontex (2013b) 'Strategic Analysis', <http://frontex.europa.eu/intelligence/strategic-analysis>

Fuerth, Leon S (2009) 'Foresight and anticipatory governance', *Foresight* 11, 14-32

Future Group (2008a) 'Informal JHA Council on 25/26 January 2008. Report of the High Level Advisory Group on the Future of EU Home Affairs Policies', <http://www.statewatch.org/news/2008/jan/eu-future-group-report.pdf>

Future Group (2008b) 'Freedom, Security, Privacy – European Home Affairs in an open World. Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy („The Future Group"), June 2008', <http://www.statewatch.org/news/2008/jul/eu-futures-jha-report.pdf>

George, Roger Z (2008) 'The Art of Strategy and Intelligence' in Roger Z George, James B Bruce (eds) *Analyzing intelligence: origins, obstacles, and innovations* (Washington, D.C.: Georgetown University Press), 107-121

Glenn, John (2013) 'In the aftermath of the financial crisis: risk governance and the emergence of preemptive surveillance', *Review of International Studies*, *FirstView* Article, July, 1-20, <http://journals.cambridge.org/abstract_S0260210513000132>

Grusin, Richard (2010) *Premediation: Affect and Mediality After 9/11* (Basingstoke and New York: Palgrave Macmillan)

Gruszczak, Artur (2008) 'Networked Security Governance: Reflections on the E.U.'s Counterterrorism Approach', *Journal of Global Change and Governance* 1, 1-23

Gruszczak, Artur (2009) 'Governing Internal Security in the European Union', *Central European Journal of International & Security Studies* 3, 86-103

Gruszczak, Artur (2013) 'EU Intelligence-led Policing: The Case of Counter-terrorism Cooperation' in Maria O'Neill, Ken Swinton and Aaron Winter (eds) *New Challenges for the EU Internal Security Strategy* (Newcastle upon Tyne: Cambridge Scholars Publishing), 16-39

Guiora, Amos N (2008) 'Anticipatory Self-Defence and International Law — A Re-Evaluation', *Journal of Conflict & Security Law* 13, 3-24

Gutwirth, Serge, Yves Poullet and Paul De Hert (eds) (2010) *Data Protection in a Profiled World* (Dordrecht: Springer Science)

Hebenton, Bill and Toby Seddon (2009) 'From Dangerousness to Precaution. *Managing Sexual and Violent Offenders in an Insecure and Uncertain Age', British Journal of Criminology,* 49, 343-362

Hildebrandt, Mireille and Serge Gutwirth (eds) (2008) Profiling the European Citizen. Cross-Disciplinary Perspectives (Dordrecht: Springer Science)

Hooper, Barabara (2004) 'Ontologizing the borders of Europe' in Olivier Kramsch, Barbara Hooper (eds) *Cross-Border Governance in the European Union (*London and New York: Routlesge), 209-229

Huysmans, Jef (ed) (2006) *The Politics of Protection. Sites of insecurity and political agency* (Abingdon and New York: Routledge)

Huiskamp, Gerard (2004) '*Minority Report* on the Bush Doctrine', *New Political Science* 26, 369-415

Jablonowski, Mark (2006) *Precautionary Risk Management. Dealing with Catastrophic Loss Potentials in Business, the Community and Society* (Basingstoke and New York: Palgrave Macmillan)

Johnston, Rob (2005) *Analytic Culture in the US Intelligence Community* (Washington, DC: The Center *for the* Study *of* Intelligence)

Kaunert, Christian (2010) *European Internal Security - towards supranational governance in the Area of Freedom, Security and Justice?* (Manchester: Manchester University Press)

Kaunert, Christian and Sarah Léonard (2010) 'After the Stockholm programme: an area of freedom, security and justice in the European Union?', *European Security* 19, 143-149

Kegley, Charles W Jr and Gregory A Raymond (2003) 'Preventive War and Permissive Normative Order', *International Studies Perspectives* 4, 385-394

Kölbel, Ralf and Susanne Selter (2010) 'Hostile Intent – the Terrorist's Achilles Heel? Observations on Pre-Crime Surveillance by Means of Thought Recognition', *European Journal of Crime, Criminal Law and Criminal Justice* 18, 237-259

Krahn, Timothy, Andrew Fenton and Letitia Meynell (2010) 'Novel Neurotechnologies in Film - A Reading of Steven Spielberg's *Minority Report*', *Neuroethics* 3, 73-88

Lee, Thomas H (2004) 'International Law, International Relations Theory, and Preemptive War: The Vitality of Sovereign Equality Today', *Law and Contemporary Problems* 67, 147-167

Lerner, K Lee and Brenda Wilmoth Lerner (2004) 'Tradecraft' in K Lee Lerner and Brenda Wilmoth Lerner (eds) *Encyclopedia of Espionage, Intelligence, and Security* (Detroit: Thomson Gale), vol. 3, 167.
Litwak, Robert S (2002-03) 'The New Calculus of Pre-Emption,' *Survival* 44, 53–80

Lowenthal, Mark M (2008) *Intelligence: From Secrets to Policy* (Washington, D.C.: CQ Press), 4th ed

Löfstedt Ragnar E (2005) *Risk management in post-trust societies* (Basingstoke and New York: Palgrave Macmillan)

Luban, David (2004) 'PreventiveWar', *Philosophy & Public Affairs*, 32, 207–48

McCulloch, Jude and Sharon Pickering (2009) 'Pre-Crime and Counter-Terrorism. Imagining Future Crime in the "War on Terror"', *British Journal of Criminology* 49, 628-645

Meisels, Tamar (2008) *The Trouble with Terror. Liberty, Security, and the Response to Terrorism* (Cambridge: Cambridge University Press)

Müler-Wille, Björn (2006) 'Intelligence and Democratic Accountability: A Blessing, not a Curse', *European Security* 15, 491-506

Müller-Wille, Björn (2008) 'The Effect of International Terrorism on EU Intelligence Co-operation', *Journal of Common Market Studies* 46, 49–73

Mythen, Gabe and Sandra Walklate (2010) 'Pre-crime, regulation, and counter-terrorism: interrogating anticipatory risk', *Criminal Justice Matters* 81, 34-36

Neyland, Daniel (2009) 'Who's Who?: The Biometric Future and the Politics of Identity', *European Journal of Criminology* 2009, 6, 135-155

Norman, Thomas L (2010) *Risk Analysis and Security Countermeasure Selection* (Boca Raton – London – New York: CRC Press)

Northouse, Clayton (ed) (2006) *Protecting What Matters. Technology, Security, and Liberty since 9/11* (Washington, DC: Brookings Institution Press)

Nunzi, Alfredo (2007) 'Exchange of information and intelligence among law enforcement authorities a European Union perspective', *Revue internationale de droit pénal* 78, 143-151

Occhipinti, John D (2003) *The Politics of EU Police Cooperation. Toward a European FBI?* (Boulder, CO and London: Lynne Rienner)

Omand David, Jamie Bartlett and Carl Miller (2012) 'Introducing Social Media Intelligence (SOCMINT)', *Intelligence and National Security* 27, 801-823

Poli, Roberto (2010) 'An introduction to the ontology of anticipation', *Futures* 42, 769–776

Power, Michael (2007) *Organized Uncertainty. Designing a World of Risk Management* (Oxford: Oxford University Press)

Richelson, Jeffrey T (2012) *The U.S. Intelligence Community* (Boulder, CO: Westview Press), 6th ed

Shue Henry and David Rodin (2007) Preemption. *Military Action and Moral Justification* (Oxford and New York: Oxford University Press)

Solove, Daniel J (2004) *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press)

Solove, Daniel J (2011) *Nothing to Hide. The False Tradeoff between Privacy and Security (*New Haven & London: Yale University Press)

Steele, Robert David (2002) *The New Craft of Intelligence. Personal, Public, & Political* (Oakton, VA: OSS International Press)

Treverton, Gregory F (2009) *Intelligence for an Age of Terror* (Cambridge and New York: Cambridge University Press)

Treverton Gregory F and C Bryan Gabbard (2008) *Assessing the Tradecraft of Intelligence Analysis* (Santa Monica, CA: RAND Corporation)

UK Presidency (2005) 'A European Criminal Intelligence Model', paper issued by the 2005 UK Presidency of the EU

UNODC (2011) *Criminal Intelligence. Manual for Analysts* (New York: United Nations)

Van Brackel, Rosamunde and Paul De Hert (2011) 'Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies', *Cahiers Politiestudies* 20, 163-92

Van Duyne, Petrus C (2007) 'OCTA 2006: the unfulfilled promise', *Trends in Organised Crime* 10, 120–128

Vaughan-Williams, Nick (2008) 'Borderwork beyond Inside/Outside? Frontex, the Citizen–Detective and the War on Terror', *Space and Polity* 12, 63–79

Vellani, Karim H (2007) *Strategic Security Management. A Risk Assessment Guide for Decision Makers* (Amsterdam: Elsevier)

Vidalis, Stilianos (2003) 'A Critical Discussion of Risk and Threat Analysis Methods and Methodologies', <http://www.comp.glam.ac.uk>

Waldron, Jeremy (2003) 'Security and Liberty: The Image of Balance', *The Journal of Political Philosophy* 11, 191–210

Weber, Cynthia (2005) 'Securitising the Unconscious: The Bush Doctrine of Preemption and *Minority Report'*, *Geopolitics* 10, 482-99

Wiener, Antje (2008) 'European Responses to International Terrorism: Diversity Awareness as a New Capability?', *Journal of Common Market Studies* 46, 195-218

Winn, Neil (2003) 'The European Union's External Face: The 'Europeanisation' of JHA and CFSP', *Perspectives on European Politics and Society* 4, 147-166

Wortley, Richard and Matthew McFarlane (2011) 'The role of territoriality in crime prevention: A field experiment', *Security Journal* 24, 149–156

Xu, Mark (ed) (2007) *Managing strategic intelligence: techniques and technologies* (Hershey and New York: Information Science Reference)

Yoe, Charles (2012) *Primer on Risk Analysis. Decision Making Under Uncertainty* (Boca Raton, FL: CRC Press)

Zedner, Lucia (2007) 'Pre-Crime and Post-Criminology?' , *Theoretical Criminology* 11, 261–81

Zedner, Lucia (2010) 'Pre-crime and pre-punishment: a health warning', *Criminal Justice Matters* 81, 24-25

Zoutendijk, Andries Johannes (2010) 'Organised crime threat assessments: a critical review', *Crime, Law and Social Change* 54, 63-86