NEW SECURITY CHALLENGES
Series Editor: Stuart Croft

Intelligence Security in the European Union

Building a Strategic Intelligence Community

Artur Gruszczak

New Security Challenges

Series Editor

Stuart Croft
Professor of International Security
Department of Politics and
International Studies
University of Warwick, UK

Director
ESRC's New Security Challenges Programme
Warwick, UK

The last decade has demonstrated that threats to security vary greatly in their causes and manifestations and that they invite interest and demand responses from the social sciences, civil society, and a very broad policy community. In the past, the avoidance of war was the primary objective, but with the end of the Cold War the retention of military defence as the centrepiece of international security agenda became untenable. There has been, therefore, a significant shift in emphasis away from traditional approaches to security to a new agenda that talks of the softer side of security, in terms of human security, economic security, and environmental security. The topical New Security Challenges series reflects this pressing political and research agenda.

More information about this series at
http://www.springer.com/series/14732

Artur Gruszczak

Intelligence Security in the European Union

Building a Strategic Intelligence Community

palgrave
macmillan

Artur Gruszczak
Jagiellonian University
Krakow, Poland

New Security Challenges
ISBN 978-1-137-45511-6   ISBN 978-1-137-45512-3 (eBook)
DOI 10.1057/978-1-137-45512-3

Library of Congress Control Number: 2016942740

Cover illustration © Deco / Alamy Stock Photo

Printed on acid-free paper

This Palgrave Macmillan imprint is published by Springer Nature
The registered company is Macmillan Publishers Ltd. London

To my beloved children Gabriela, Monika and Filip

Acknowledgments

Doing research in so sensitive and politically charged an area as international intelligence cooperation is by no means an easy task. Yet it was clear from the outset that there would be a significant contrast between the academic stance adopted by the present author and the political and security interests of officials and decision makers. A research project on intelligence security in the European Union would bring with it many difficulties and challenges.

For a civilian representative of academia, access to data is always challenging. The general content and many details of intelligence organisations and processes remain closely guarded by state agencies and subject to strict legal regulations. The veil of secrecy is often totally opaque. Grappling with uncertainty and the knowledge gaps emerging in the course of the research was often a frustrating activity. I was fortunate enough to receive help from many people during the preparation of this book.

The book is not only the result of the study of literature, documents, reports and publications. It owes its existence to the many officials and experts who were willing to hold conversations with me and share their expertise and knowledge. They were representatives of EU institutions and agencies, intelligence officers (civilian and military) of some Member States, and law-enforcement officers from selected EU countries. I hope it is not a breach of confidence to thank them for their great help, patience and consideration. I recognise and appreciate that they agreed to semi-structured interviews in spite of the sensitivity of the issues raised in our conversations. I thank them for their confidence and the time they devoted to my project.

Some interviewees were official representatives of institutions, agencies or offices involved in EU security policy or the national security of Member States. I would like to express my thanks to Ilkka Salmi, José Miguel Palacios-Coronel, Gilles de Kerchove, Oliver Rajan, Oliver Luyckx, Jamie Shea, Juliette Bird and Paul Minnebo.

Special thanks for help in arranging meetings with EU officials and for critical comments on some parts of the manuscript go to Piotr Rakowski, Michał Narojek, Mark Rhinard and Tom Delreux.

I would also like to thank an array of experts and academic colleagues for taking the time to respond to my queries with information, advice and sometimes friendly scepticism. Among those to whom I owe a debt of gratitude for their assistance are Peter Gill, Mark Phythian, Monica den Boer, Raphael Bossong, Oldřich Bureš, Filip Jasiński, Fernando Velasco Fernández, Javier Argomaniz, Maria O'Neill, Rubén Arcos, Diego Navarro Bonilla, Antonio Díaz Fernández, Oscar Jaime Jiménez, Glen Segell, Sarah Wolff, Karolina Pomorska, Cyrille Fijnaut and Toine Spapens.

Last but not least, I am particularly indebted to an EEAS official who preferred to remain anonymous. His inspiring comments, suggestions and opinions led to a much-improved final result.

I would like to emphasise that the opinions and views expressed in this book are exclusively my own. Any errors remain my sole responsibility.

The bulk of the work on this book was undertaken within the research project 'The European intelligence community *in statu nascendi*'. I gratefully acknowledge the financial support of the Polish National Science Centre (grant no. DEC-2011/01/B/HS5/00961).

I am particularly grateful to Palgrave's editors Eleanor Davey Corrigan, Hannah Kaspar and Sarah Roughley for their endless patience and professionalism. I also wish to thank Garry Robson for his valuable linguistic assistance.

Finally, I would have not been able to keep myself motivated throughout the researching and writing of this book without the help, patience and support of my wife Karolina, my daughters Gabriela and Monika, and my son Filip.

Artur Gruszczak
October 2015

Contents

Abbreviations

AFSJ	Area of Freedom, Security and Justice
ARA	Annual Risk Assessment
ATSA	Aviation and Transportation Security Act
AWF	Analysis Work File
CBRN	chemical, biological, radiological and nuclear
CCA	Crisis Coordination Arrangements
CFSP	Common Foreign and Security Policy
CIA	Central Intelligence Agency
CIRAM	Common Integrated Risk Analysis Model
CIS	Customs Information System
CMS	case management system
CoOL	Consular Online
COREPER	Committee of Permanent Representatives
COREU	Correspondence Européenne
COSI	Standing Committee on Operational Cooperation on Internal Security
COSPOL	Comprehensive Operational Strategic Planning for the Police
CRS	Crisis Response System
CSDP	Common Security and Defence Policy
CYBERINT	cyber intelligence
DG	Directorate-General
EC	European Community
EC3	European Cybercrime Centre
ECIM	European Criminal Intelligence Model
EDA	European Defence Agency
EEAS	European External Action Service
EEC	European Economic Community

ELINT	electronic intelligence
ENISA	European Union Agency for Network and Information Security
EPC	European Political Cooperation
ESDP	European Security and Defence Policy
ESS	European Security Strategy
EU	European Union
EUMS	European Union Military Staff
EUMS INT	Intelligence Directorate of the EU Military Staff
EUROSUR	European Border Surveillance System
EUSR	European Union Special Representative
FRAN	Frontex Risk Analysis Network
FASP	foreign affairs and security policy
FSJ	freedom, security and justice
GEOINT	geospatial intelligence
GMES	Global Monitoring for Environment and Security
GSC	General Secretariat of the Council
HR/VP	High Representative/Vice-President
HUMINT	human intelligence
IMINT	imagery intelligence
INTCEN	Intelligence Analysis Centre
INTDIV	Intelligence Division
IPCR	Integrated Political Crisis Response
ISAA	Integrated Situational Awareness and Analysis
ISB	Intelligence Steering Board
ISS	Internal Security Strategy
ISTAR	intelligence, surveillance, target acquisition and reconnaissance
IWG	Intelligence Working Group
JHA	justice and home affairs
LIBE	Committee on Civil Liberties, Justice and Home Affairs
MASINT	measurement and signature intelligence
MEP	Member of European Parliament
MIC	Monitoring and Information Centre
MD	VII Department for Crisis Response and Operational Coordination
MMT	mission monitoring team
MS	Member State
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organisation
NCC	National Coordination Centre
NGO	non-governmental organisation
NSA	National Security Agency
NTA	New Transatlantic Agenda

OCTA	Organised Crime Threat Assessment
OPS WAN	Operations Wide Area Network
OSCE	Organisation for Security and Co-operation in Europe
OSINT	open-source intelligence
PIR	prioritised intelligence requirements
PNR	passenger name record
PPWEU	Policy Planning and Early Warning Unit
PROTINT	protected information intelligence
PSC	Political and Security Committee
RAU	Risk Analysis Unit
RELEX	External Relations
RESINT	research-originating intelligence
RMA	Revolution in Military Affairs
SAR	synthetic aperture radar
SATCEN	EU Satellite Centre
SCAN	scanning, analysis and notification
SIAC	Single Intelligence Analysis Capacity
SIGINT	signals intelligence
SIS	Schengen Information System
SITCEN	Joint Situation Centre
SITINT	situational intelligence
SitRoom	EU Situation Room
SOCINT	socio-cultural intelligence
SOCMINT	social media intelligence
SOCTA	Serious and Organised Crime Threat Assessment
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TECHINT	technical intelligence
TE-SAT	Terrorism Situation and Trend Report
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TFTP	Terrorist Finance Tracking Program
TWP	Terrorism Working Party
UK	United Kingdom
UN	United Nations
USA	United States of America
VIH	virtual intelligence hub
VIS	Visa Information System
WEU	Western European Union
WKC	Watch-Keeping Capability
WMD	weapon of mass destruction
WWII	Second World War

CHAPTER 1

Introduction

Outline of the Problem

Intelligence has become one of the most telling aspects of national and global security in the twenty-first century. Its role in public affairs, the private sphere, security strategies and policies, even in commercial relations and social media, has grown and expanded immensely (Scott and Jackson 2004, p. 1; Jackson and Siegel 2005, p. 1; Scott and Hughes 2011, p. 6). Much of this phenomenon can be attributed to the rapid civilisational, cultural, psychological and technological transformations of the last quarter of a century. They have brought about enormous progress and modernisation in many parts of the world but have also provoked grievance, rebellion and a feeling of marginalisation among the masses populating underdeveloped regions. The lost sense of community, multidimensional cleavages between nations, communities and social groups, and concern about the future have contributed to uncertainty, anxiety and distrust among the host of actors populating the global arena. In this gloomy scenario, intelligence emerges as a factor contributing to the reduction of uncertainty and to the improvement of situational as well as strategic knowledge about the facts, concepts and principles that apply in a given realm (De Jong and Fergusson-Hessler 1996, p. 105; Fingar 2011, pp. 4–6).

A. Gruszczak, *Intelligence Security in the European Union*,
DOI 10.1057/978-1-137-45512-3_1

The broad application of the concept of intelligence is a feature of today's world. Intelligence is a means to an end and this end is security (Gill and Phythian 2006, p. 1). Hence, it naturally sparks the growing interest of statespersons, decision makers and scholars fascinated by the expansion of intelligence disciplines, the increased relevance of information and knowledge, and the growing significance of technological drivers, as well as public officials and social activists who are afraid of information overload, declining standards of intelligence activities, the widening margins of error in intelligence analysis and even the potentially devastating impact of these factors on decision making and democratic governance. It is hard to imagine a strong, robust, effective government without a tailor-made knowledge management apparatus ancillary to the state and society. The importance of knowledge management, information analysis, data processing and intelligence has been a notable feature of government policies and world politics, particularly since 9/11 and subsequent terrorist attacks all over the world. National security policies and international security cooperation arrangements have begun to highlight growing reliance on early warning, situational awareness, threat assessment and risk analysis. To be effective, these methods need reliable, accurate and precise data and information. Given the immense amount and huge diversity of the information available, selecting, processing and adjusting it to policy requirements and decision-making procedures has become absolutely indispensable. Intelligence has come to play a pivotal role in contemporary security policies and can determine governments' resilience to threats and hazards.

The latter aspect underpins the present study. Despite the immense proliferation of intelligence methods, means and tools, states have maintained their predominance in the realm of information gathering, processing and analysis, especially with reference to the strategic objectives of their governments and the vital security interests of their societies. In the face of growing competition from private actors offering valuable intelligence products based on open sources, states have widened the scope of their intelligence activities, applying modern technologies to create a variety of end products. They are also aware that the growing interconnectivity of information sources may bring about both positive and negative outcomes. The collection, processing and sharing of available information and data to enhance internal security and preserve public order can stimulate various forms of cooperation. Yet it also may cause the consolidation of existing 'spaces of insecurity' (Ingram and Dodds 2009, pp. 1–12;

Grenfell and James 2009, pp. 3–19), generating crime, violence and conflict. Moreover, it may induce certain dysfunctional actors (individuals, groups, organisations) to engage in hostile activities undermining public order, attacking state institutions and threatening populations.

Contemporary intelligence must cope adequately with the complexity, diversity and wide range of activities undertaken by countless participants in public life. Accurate intelligence is essential for effective and legitimate security management and is equally important for organisational performance. This rule is binding on both states and international organisations. This book deals with intelligence activities undertaken by the latter. Although international organisations act beyond the traditional supremacy of the sovereign state, this category of international actor is not excluded from intelligence activities. Though largely dependent upon the resources and expertise of their member states, several intergovernmental organisations have successfully developed intelligence capabilities and even managed to hold their own assets. In principle, these are the organisations dealing with regional or global security, including its military and crisis-management aspects, such as the United Nations (Smith 1994; Dorn 1999, 2010; de Jong et al. 2003; Steele 2006), NATO (Laino 2011, pp. 13–14; Kriendler 2013) and the European Union.

Current security challenges for the European Union as an international organisation and as a community of Member States require a consistent, proactive, intelligence-led response. This politically motivated objective has to be shared by EU institutions and agencies and should engage Member States in a more intense form of cooperation. Hence data exchange, intelligence sharing and intelligence-led operations make up a specific security *Zeitgeist* which inspires national and supranational counterparts to make stronger efforts and invest their resources in the creation of a strategic intelligence community within the EU. Recent developments have only served to prove the well-known principle of knowledge dominance in the realm of security and made the public aware of the size, scope and depth of state policies in this regard. The EU is no exception: the proposals and initiatives it has undertaken in recent years were timely and adequate to the emerging problems of information analysis, knowledge management and intelligence sharing. The proliferation of threats to security demands a functional intelligence architecture. The European Union has responded to this challenge by gradually developing connections and linkages between the relevant authorities of the Member States and systematically engaging available EU agencies and bodies in intelligence-led cooperation.

Intelligence as an Element of EU Security Cooperation

The very word 'intelligence' has not been in vogue in Brussels. 'Intelligence' seemed to be limited to national use, identified with specific activities such as secret operations, eavesdropping or just spying. 'Information' was a politically neutral term and as such was easily accepted by the European Community's institutions and introduced into communication channels at EU level. For example, in the La Gomera declaration, adopted at an informal meeting of the Ministers for Justice and Home Affairs of EU Member States convened in 1995 in the face of the growing terrorist menace, there was a reference to a 'need for thorough coordination between Member States by way of improved machinery for police and judicial cooperation, through an increase in exchange of operational information about terrorist groups' (Council of the EU 1995).

Before 9/11, 'intelligence' seldom appeared in EU documents and related policies but was used in describing police cooperation through the European Police Office, Europol. The acquisition, collation and analysis of information and intelligence as well as the provision of strategic intelligence were among Europol's tasks. It was also mentioned by the Western European Union (WEU) as a defence component of the EU. Following the 1992 adoption of the Treaty on European Union (TEU), which contained provisions on foreign, security and defence policies, some initiatives were endorsed for the development of the operational role of the WEU as defined in the Petersberg declaration of 1992. Little attention was paid to intelligence at that time; nevertheless at the Extraordinary Council of Ministers of the WEU in 1995 a Common Concept of European Security was adopted, entailing intelligence capabilities developed in an Intelligence Section and a Satellite Centre set up within WEU's institutional structure (WEU 1995a). The meaning of 'intelligence' as an element of EU security policy was taken for granted by Member States and as such was excluded from deliberations in supranational institutions.

In the aftermath of 9/11, 'intelligence' became synonymous with an effective and comprehensive response to the global terrorist threat. However, it still lacked a precise definition and was largely identified with information exchange between the security and intelligence services of EU Member States and overseas partners. The terrorist attack in Madrid on 11 March 2004 forced EU institutions and Member States to accelerate and widen anti-terrorist cooperation, including national intelligence services and relevant EU bodies, especially Europol and the Joint Situation Centre (SITCEN). By the same token, there was a growing need for an official interpretation of what constituted information and what constituted intelligence for the purpose of developing cooperation within the legal and institutional framework of the EU.

The first attempt at a single definition of intelligence was made by the Commission of the European Communities. In the 2004 Commission communication on enhancing access to information for law-enforcement agencies, there was an odd remark (added, by the way, in a footnote): 'For the purpose of this Communication the expression "data" or "information" means "data, information and intelligence" unless otherwise indicated; the term "intelligence" refers to "criminal intelligence".' (Commission of the EC 2004, p. 5). Such imprecise wording did not facilitate efforts to work out a cohesive approach to EU cooperation on exchanging information and data relevant to cross-border activities of law-enforcement agencies. Incentives for the specification of the meaning of intelligence in EU policy were included in the European Council multi-annual programme of strengthening the area of freedom, security and justice, adopted in November 2004. In 2006 the Council, acting on the initiative of Sweden, adopted Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between the law-enforcement authorities of Member States. Article 2(d)(i) of the Framework Decision includes the following peculiar provision:

> information and/or intelligence:
>
> - any type of information or data which is held by law-enforcement authorities; and
> - any type of information or data which is held by public authorities or by private entities and which is available to law-enforcement authorities without the taking of coercive measures [...]. (Council of the EU 2006c, p. 91)

A question remained as to whether this definition provided a precise and operational meaning of intelligence. As many experts emphasise, information is not synonymous with intelligence. Information and data are raw materials, while intelligence is processed information and data cross-checked against other available sources of information and knowledge. From the functional standpoint, criminal intelligence executed at the national level used to be identified with supporting evidence-led inquiry: gathering information for a police investigation, structuring the evidence for courts or revealing the nature of criminal phenomena. International collaboration in criminal justice involves strategic intelligence: evaluation of threats, assessment of criminality's impact, and anticipation of future threats and risks. EU experience has proved the viability of the strategic dimensions of criminal intelligence given the limitations on operational activities and barriers maintained by the respective national authorities with regard to data sharing and information exchange.

Whether or not the definition of intelligence contained in the Swedish Framework Decision was useful, it introduced a highly important functional division between (i) criminal intelligence for EU internal security and criminal justice and (ii) military and socio-political intelligence falling under the EU Common Foreign and Security Policy. Further interpretations followed a debate in late 2013 over the prospects for the establishment of an EU intelligence agency. Top officials representing the European Commission and the EU Intelligence Analysis Centre (INTCEN) presented a common position on the grounds of the Treaty of Lisbon. They recalled that Article 4.2 of the TEU stipulated that the Union respects the 'essential functions of its Member States, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.' (European Union 2012, p. 18). Ilkka Salmi, the director of INTCEN, emphasised that 'The Lisbon Treaty clearly states that national security is the competence of the member states. And that's of course interpreted in many member states as to include intelligence—in my understanding as well. Only from the legal point of view, it would mean that we would need a treaty change' (Clerix 2014).

Substantial arguments went in hand with the official denial of the possibility of establishing an EU intelligence institution. This position was articulated in the late 2000s and reflected opinions that had already been formulated by former officials and experts in the 1990s. William Shapcott, former director of the EU Joint Situation Centre, said: 'the EU itself has no intelligence agency of its own, no secret intelligence assets, and that therefore many of the features of the traditional intelligence cycle are absent or only present in a very distorted form' (Shapcott 2011, p. 118). Brigadier General Günter Eisl, former Intelligence Director at the European Union Military Staff, added: 'We have a very colourful patchwork of organisations at member state level. There is no single model: each has developed based on historical and cultural experiences' (SDA 2011). The establishment of a single EU intelligence agency was out of the question. The High Representative for the Common Foreign and Security Policy (CFSP) declared several times that formal institutionalisation and centralisation of intelligence cooperation at EU level was not feasible.

Such a fundamental stance on the part of the Commission and the High Representative does not, however, exclude the possibility of the institutionalisation of various forms of cooperation in the field of data collection, analysis and intelligence sharing. Intelligence roles are performed by certain EU agencies (Europol, Frontex, the EU Satellite Centre, the European Maritime Safety Agency). It should also be acknowledged that numerous units embedded in the European External Action Service (EEAS) structure (the EU Intelligence Analysis Centre, the Intelligence Directorate of the EU Military Staff) are also tasked with intelligence gathering, processing and sharing. Interestingly, Boin, Ekengren and Rhinard identified a wide array of EU institutional settings and working arrangements comprising 84 systems and tools dedicated to gathering, analysing and sharing information (Boin et al. 2014). Such a plethora of agencies, bodies, systems and solutions requires a certain level of coordination. The European Commission, in March 2011, highlighted the need to integrate the activities of the EU agencies responsible for collecting, processing and exchanging information and intelligence. But it did not imply the need for a single institutional framework.

Rather, intelligence security cooperation in the EU has been focused on establishing new and reinforcing existing forms of networked cooperation and coordination in the field of information analysis and intelligence production and sharing. Moreover, in some sensitive areas, like counter-terrorism, the fight against organised crime and cyber-criminality, EU agencies and units have taken advantage of intergovernmental arrangements worked out by certain Member States outside the legal-institutional framework of the European Union. It was taken for granted that the operational efficiency and political legitimacy of these activities require the reinforcement of European intelligence cooperation on a basis of systemic interoperability, availability and loyalty.

This conviction reflects the evolution of the concept of an 'intelligence community' within the European Union seeking to strengthen systematic cooperation between Member States based on EU law, in the belief that permanent or potential threats interfering in and destabilising the security of the Union could be reduced to a minimum given closer cooperation between national intelligence services and the active engagement of relevant EU agencies and bodies.

Scholarship on EU Intelligence Cooperation

The flurry of writing about intelligence activities, even in the post-9/11 mood, has not seen any special emphasis on EU intelligence cooperation. Scholars working in intelligence studies have focused on 'big issues', like intelligence failures (Betts 2007; Turner 2005; Zegart 2005, 2006; Hulnick 2006b; Jervis 2010; Jones and Silberzahn 2013; Dahl 2013), reforms of national intelligence communities (Rovner and Long 2005-6; Posner 2005; Pillar 2011), oversight and accountability of intelligence services (Born et al. 2005; Born and Caparini 2007) and technological aspects of intelligence (Ferris 2004).

The topic of intelligence cooperation within the European Union seemed fairly exotic in mainstream intelligence studies of the last decade of the twentieth century (Berkowitz and Goodman 1989; Richelson 1990; Gries 1991; Hulnick 1991). However, the Maastricht Treaty gave a strong impetus to thinking about European security in the new institutional context. Hence, some insightful observers of the dynamics of EU integration argued that intelligence cooperation should be one of the fundamentals of security policies in the European Union and that appropriate institutions and mechanisms should be set up to make intelligence sharing plausible (Donath 1993; Klerks 1993).

Noticeable progress in the late 1990s, especially the emergence of the first intelligence units within the EU's security and defence policy, encouraged the WEU's Institute for Security Studies to organise research on the intelligence policy of the European Union. Given that the initial forms of strategic intelligence cooperation were developed within the WEU structures, the research by a group headed by Alessandro Politi should be considered as a sort of politically driven evaluation of the purposes, resources, capabilities and prospects for a full-fledged EU intelligence cooperation (Politi 1998a). What was important in Politi's research was that it also embraced what was then third-pillar cooperation, focused on internal security and border management. This field of security cooperation and intelligence sharing was already being studied in the early 1990s, although the research results were often either fragmentary or superficial (Bonnefoi 1994; Robertson 1994; Bigo 1995; Hebenton and Thomas 1995). Politi indicated that the EU could and should develop two types of intelligence analysis: strategic military intelligence, aimed at supporting the emerging security and defence policy; and criminal intelligence, which sought to enhance the effectiveness of the law enforcement and border protection of EU territory and the Schengen area (Politi 1997, 1998a).

At the turn of the century, a paper published by Ole Villadsen, a graduate fresh from Georgetown University, summed up the developments in EU cooperation in the 1990s and highlighted incentives for a genuine European intelligence policy (Villadsen 2000). Post-9/11 developments in the global and EU security environments stimulated the debate around EU intelligence prospects and capacity building. Although the theme of intelligence sharing in most cases appeared in the context of the prevention of and fight against terrorism, several papers published at that time offered a macro perspective on EU intelligence processes, assessing critically its strengths and weaknesses, or better, incentives and barriers to the progress of cooperation in information exchange and intelligence sharing (den Boer 2002; Müller-Wille 2002; Messervy-Whiting 2004; Coosemans 2004). Studies and analyses of intelligence cooperation within the EU, as well as liaison between the Union and its external partners, especially the USA, mushroomed in the wake of the tragic events mentioned above (Lefebvre 2003; Reveron 2006; Sims 2006; Walsh 2006, 2007; Hertzberger 2007; Rüter 2007; Müller-Wille 2008; Dorn 2008; Svendsen 2008a, 2008b; Jeffreys-Jones 2007, 2009, 2011; Brady 2009; Baker 2010; Fägersten 2008, 2010; Tuzuner 2010; Aldrich 2011). The slow-motion character of EU initiatives, decisions and procedures dampened the initial ardour for in-depth research on intelligence cooperation in the EU.

Undoubtedly Björn Müller-Wille's analytical paper published by the EU Institute for Security Studies (Müller-Wille 2004) was the most comprehensive, insightful and informative contribution to this debate produced at that time. What is more, Müller-Wille's analysis set the direction for further research in intelligence cooperation and was a point of reference for many debates or projects related to EU intelligence capabilities and prospects. Building on an earlier article (Müller-Wille 2002), he made a thorough assessment of the various dimensions of intelligence support for EU security policy: military, law-enforcement, diplomatic, economic and crisis-management. In the final part of the paper, he put forward a model for an EU intelligence community taking the form of a specific institutional architecture involving relevant EU agencies and an intelligence communication network (Müller-Wille 2004, pp. 37–44; also Coosemans 2004). Müller-Wille's remarkable work has stood the test of time, even though after the 2004 Madrid terrorist bombing the topic of intelligence cooperation in the EU was further explored by scholars, officials and practitioners (Nomikos 2004, 2005; Vaz Antunes 2005; Duke 2006; Rüter 2007; Wetzling 2008).

The evolution of an EU security area marked by legal changes, strategic guidelines, institutional reforms and policy-making patterns stimulated theoretical and practical reflection on the impact of intelligence cooperation on the security of the Union. The search for new approaches and novel theoretical and analytical concepts introduced some interesting proposals. Adam Svendsen (2010, 2011) developed a thesis about the increased regionalisation of intelligence in Europe. Peter Gill (2006, p. 41) emphasised transnational network structuring in Europe focused on surveillance and security governance.

Björn Fägersten put forward a rational-choice model to explain why EU Member States were more or less likely to co-operate on intelligence issues. His conceptual proposal assumed that genuine and effective intelligence cooperation is feasible when intelligence and policy gains are properly balanced against autonomy and vulnerability costs at the level of state interests. If balance is produced, it is determined by critical drivers and peripheral factors—both enablers and barriers—further influencing prospects for effective intelligence cooperation (Fägersten 2008). Fägersten deployed the institutionalist perspective in another analytical paper related to Europol's intelligence capacity (Fägersten 2010), using organisational/institutional and cultural arguments to develop the concept of bureaucratic resistance to wide-ranging international intelligence cooperation. In a recent paper (Fägersten 2014), he highlighted the principle of institutional interconnectedness as a constitutive element of European intelligence cooperation. The problem of the bureaucratisation of EU intelligence cooperation was also raised by Thomas Jäger and Anna Daun (2009). They adopted the principal–agent theory to highlight the potential traps that exist in complex organisational frameworks.

James Igoe Walsh opposed the institutional perspective proposed by Müller-Wille and Fägersten. He argued that cultural and psychological determinants, most of all trust, are crucial for effective intelligence sharing in the EU. He mentioned several bodies engaged in intelligence cooperation, namely Europol, the Club of Berne and the EU Military Staff, and highlighted their roles as facilitators of intelligence collaboration. He acknowledged their positive contribution to technical mechanisms and channels for the diffusion of intelligence among national services. However, he also pointed to the constant deficit of trust among national stakeholders as a critical factor undermining effective intelligence sharing (Walsh 2006).

Nicholas Dorn's reflection on the opportunities and prospects for EU intelligence cooperation was based on the assumption that the establishment and development of this intelligence cooperation can occur at a strategic level and should mainly address various forms of international criminality. Hence, the context of this cooperation should involve cultural, psychological, educational, economic and sociological factors. Dorn suggested that the 'EU should encourage a security model of public-private partnership, emphasising excellence in diversity in relation to information systems, data collection, model assumptions, analytic models, and reporting' (Dorn 2008, p. 180).

Eveline R. Hertzberger offered an overall view of intelligence sharing in the EU in the context of counter-terrorism. She used the term 'EU intelligence community' with respect to four agencies and entities (Europol, SITCEN, EUMS Intelligence Division and EU SATCEN), stipulating that 'they fulfil the intelligence function for the EU, but are not intelligence services in the traditional sense of the word. Unlike national intelligence agencies, they do not have collection capabilities.' (Hertzberger 2007, p. 3). Certainly, she was wrong on this point as she missed the important open-source intelligence (OSINT) component in the everyday intelligence activities of relevant EU agencies and bodies. Focusing on EU counter-terrorism policy, Hertzberger put the emphasis on 'foreign intelligence', that is the external dimension of information gathering and intelligence sharing.

A monograph by three Spanish scholars greatly enriched the debate around the viability of EU security intelligence. Antonio Díaz Fernández, Miguel Revenga Sánchez and Oscar Jaime Jiménez (2009) placed the field of intelligence cooperation within the framework of the Europeanisation concept. They deemed this particularly useful for overcoming the dichotomies prevailing in existing scholarship in EU intelligence cooperation: intergovernmental cooperation vs supranational integration; national interests vs community objectives; transnational networks vs supranational bureaucracy (Díaz Fernández et al. 2009, pp. 56–7). This neo-functionalist approach enriched the debate with topics and threads previously neglected or marginalised, such as the overlapping of institutional arrangements, cross-referential connections between internal and external security agents and structures, and the logic of networked governance of EU intelligence actors and policies (Díaz Fernández et al. 2009, pp. 58–67).

With the growing importance of prevention, precaution and the anticipation of threats highlighted in the 2010 EU Internal Security Strategy, more scholars expressed an interest in the study of a proactive intelligence-led approach to EU security (Brady 2008; Gruszczak 2013; den Boer 2014) and a reinvigorated cooperation between Member States and EU agencies and bodies. The relationship between policing and intelligence was seen in the context of the blurring of boundaries and overlapping of powers as well as the emergence of new 'hybrid' police-intelligence institutions (Cordell 2010; Svendsen 2011, p. 537; Završnik 2013).

Mai'a K. Davis Cross's studies on a European trans-governmental intelligence network are among recent conceptual proposals in the field of EU intelligence studies. Cross bases her approach to intelligence cooperation in the EU on the concept of epistemic communities. With regard to security integration in Europe, she highlights the strong tendency towards its redefinition by specific knowledge-based networks (Davis Cross 2011, 2013a). She developed this idea in a paper devoted to INTCEN (Davis Cross 2013b), in which she argued that INTCEN is at the centre of a trans-governmental network of intelligence professionals nested in the emerging European intelligence space.

The European context of intelligence has recently attracted the attention of scholars identified with mainstream intelligence studies (Duyvesteyn et al. 2014) or EU internal security policies (Kaunert and Léonard 2013). In the latter strand, a group of experts on EU counter-terrorism have offered insightful views of the role of intelligence in the prevention and combating of terrorist threats (Balzacq and Léonard 2013; Gruszczak 2013; Argomaniz et al. 2015; den Boer 2015).

The above review of leading concepts and propositions has pointed to the growing diversity and advancement in the study of EU intelligence cooperation. Regardless of the relatively low rate of scholarly 'production', the rising quality and insightfulness of these studies assert the increasing importance of intelligence for EU security policy and strategy.

Research Problems and Hypotheses

The European Union is the world's most complex and advanced international organisation, a unique integration of sovereign nation-states and supranational institutions within a single legal and institutional framework. In the course of its evolution and transformation, it has become the organisational vehicle for numerous sub-regional, regional, national and supranational collective actors eager to align their interests and take advantage of synergies emerging on the supranational level (Watts 2008; Staab

2011; Lelieveldt and Princen 2011). As Castells (2000, pp. 362–3) wrote, 'the European member states have been forced to innovate, producing, at national, regional, and local levels, new forms and institutions of governance, including the Union itself as a "new form of state", i.e., "the network state"'. In this context, the European Union may be regarded as a networked polity (Castells 1998, p. 330; Ansell 2000). Networks are created by sets of actors involved in public governance focused on joint problem solving (Torfing 2005, pp. 306–7; Hajer and Versteek 2005, p. 341; Provan and Kenis 2007; Nutt and Pal 2011; Keast 2014, pp. 22–3). Policy networks imply a cooperative mode of governance based on stable patterns of exchange and reciprocity. Multiple actors with overlapping competences engage in cooperation and equivalent exchange.

Intelligence as an element of EU security governance is subject to the dynamics of networks which emerge in a given institutional and functional context in response to integration objectives shared by the Member States and pursued by supranational institutions. The emerging global system of interconnections entered a new stage in the early 1990s with a rapid transformation into a complex multidimensional networked construction saturated with information and data. It opened up a vast space crowded with a growing number of transnational actors, gradually extending the scope of their activities and proliferating functional and dysfunctional patterns of relations. Globalisation and networking posed new challenges to intelligence services because of the massive flood of data, often overloading contemporary intelligence systems and demanding new technical and human capabilities. The growing volume of data increased the level of uncertainty and enlarged the intelligence gap between the amount of raw material and the ability to process it (Codevilla 1992, pp. 3–6; Fingar 2011, pp. 107–8; Lorber 2015, pp. 6–7). The proliferation of threats at transnational and global levels increased pressure on national intelligence organisations, as well as law-enforcement services, towards the more efficient prevention and combating of criminal activities, particularly terrorism. The need for comprehensive knowledge, accurate and fast analyses and usable intelligence products was rising with growing demands from decision makers. In these circumstances, nation-states' security strategies and policies increasingly began to rely on sources of information located overseas, outside the scope of their jurisdiction and formal competence, the accessibility of which was subject to international, formal or tacit, agreements and deals.

The research objective of the present study is to examine the constitution, structure and management of EU intelligence networks as part of the security policies of the European Union. In particular, the aim is to investigate the ability of EU Member States, as well as the institutions and agencies responsible for security matters in the Union, to develop effective, legitimate and accountable institutions and mechanisms for the collection, transmission, processing and exchange of intelligence and other information related to its security. In this regard, synergy at the level of information exchange and intelligence is a key element that will be used as a basic indicator validating the ability to create a European intelligence community on the basis of EU law and institutions.

I argue that the European Union has provided a framework for intelligence cooperation in order to better secure its interests and build resilience to unauthorised and unrestricted surveillance and interference performed by non-EU (state and non-state) actors. I intend to show that the EU—regardless of the poor prospects for making a 'European NSA or CIA'—has been creating a specific organisational and functional structure capable of effectively performing intelligence functions.

I advance the hypothesis that the European Union, considered as a complex network of institutions and agencies located on the supranational and national levels, has been evolving towards a multidimensional complex of intersecting policy fields underpinning the ongoing process of European security integration. Security is a specific policy field in the EU given that it encompasses both loose institutional arrangements and hierarchical structures, and adaptive community actions. Security governance networks in the EU, contrary to Torfing's claims (2005, p. 307), are not self-regulating (Scharpf 1994, p. 36) but constitute a polycentric configuration of interdependent actors guided by formal and informal arrangements directed towards certain policy outcomes (Krahmann 2003; Weber et al. 2004; Kirchner and Sperling 2007; Hollis 2010; Christou et al. 2010; Mérand et al. 2011; Whelan 2012, pp. 18–24; Giumelli and Lavallée 2013; Ehrhart et al. 2014a).

Information sharing is vital for the proper functioning of the EU security complex and indispensable for effective handling of threats and risks to European security. As Ricci (2008, p. 12) observed, 'Politicians, diplomats, humanitarian workers, mediators, intelligence operatives are part of the same ecosystem, constrained by the same environmental factors. […] The whole point is the need to adapt to the environment.' Therefore, the European Union's strategic objective in the area of security is to determine a functional architecture of interconnected institutional nodes of intelligence analysis responding to the most relevant problems, challenges and risks. To meet this objective Member States, along with appropriate EU institutions and agencies, must create an intelligence community based on effective rendering of time-sensitive intelligence, sharing of best practices and analytical products, and contributing to effective and legitimate security governance in the EU.

This book builds on the hypothesis that a European intelligence community can be established at the EU level. In particular it examines strategic intelligence, that is to say the knowledge produced for EU officials in charge of security policies and actions contributing to policy making in EU institutions and agencies. Member States participate in the joint intelligence enterprise with a view to the acquisition of intelligence output for their national leaderships. The value added to intergovernmental cooperation between the intelligence services of Member States derives from the synergetic effects at the EU level produced by the special intelligence tradecraft practised by institutions and agencies.

Methodology

The present study is situated at the intersection of selected disciplines, sub-disciplines and inter-disciplinary fields that have hitherto proved their usefulness in research in the field of European security, strategic studies and intelligence cooperation. Such a cross-disciplinary approach is particularly suitable for an enquiry into strategic intelligence cooperation in the European Union. A functional merger of different disciplines and interdisciplinary fields is evidence of a holistic approach, which is particularly important in the present study. One of its fundamental objectives is to argue for the emergence of an EU intelligence community as a networked security construction of interconnected hubs focused on information analysis, knowledge management and intelligence sharing at the strategic level. The concept of an EU strategic intelligence community needs to overcome artificial divisions between academic disciplines in order to develop unorthodox methods and instruments of empirical research. Such an approach to the study of security cooperation in the EU is owes much to Monica Gariup's research on European security culture (Gariup 2009, pp. 5–6).

To avoid excessive ‘compartmentalisation’ of the theoretical foundations of the present book, it is anchored in three areas: European integration studies, intelligence studies and network science.

European integration studies have given a solid background to more specific research in security-related fields. The enormous research agenda followed since the early years of integration within the framework of the European Communities has brought about a plethora of concepts, approaches, theories and frameworks aiming to explain the increasingly complex empirical issues generated by integration processes (Mattli 1999; Rosamond 2000; Cini 2006; Chryssochoou 2009; Egan et al. 2010). Addressing the problem of intelligence cooperation within the wider context of European integration is highly demanding and risky. The dominant strands of theories and conceptual frameworks may appear only partially feasible.

Intelligence studies have been an academic discipline for quite a long time (Honig 2007, pp. 700–3; Warner 2007, pp. 21–5; Fisher and Johnston 2008; Kahn 2009, p. 4; Johnson and Shelton 2013, pp. 112–13; Agrell and Treverton 2015, pp. 14–31). Studies of intelligence have been synchronised with major events on the international stage, focusing on security, defence and prevention. After the Second World War intelligence was described as the ‘missing dimension’ in the study of international relations (Jackson and Siegel 2005, p. 2). The expansion and rapid development of intelligence studies occurred during the Cold War period (Prados 1982; Bamford 1982; Reynolds 1985/6; Richelson 1985, 1986, 1990; Richelson and Ball 1985; Freedman 1986). Post-Cold War studies in intelligence had to respond adequately to rapidly evolving international security relations and structures (Hoffman 1996; Wiebes 2003; Wirtz 2007; Gill et al. 2009). Publications on intelligence topics in the 1990s were more varied and nuanced, and began expanding towards diplomacy, international peacekeeping, public administration, information technologies, knowledge management and interception of communications (Treverton 1995; Steele 1995; Richelson 1996; Herman 1996; Hager 1996; Berkowitz 1997; Castagna 1997; Boatner 2000). They seldom touched upon the organisation, mechanisms and procedures of cooperation among national intelligence services, especially in the established framework of international organisations or arrangements (Klerks 1993; Aldrich 1995, 1998; Alexander 1998; Aid and Wiebes 2001). Moreover, they lacked a strong theoretical framework. Mark Phythian (2009, pp. 54–5) explains: ‘There seems little prospect of a unifying theory of intelligence because of the scope and complexity of the subject area and, moreover, little need in that a significant part of the frame that this would provide already exists in the form of structural realist analyses.'

Drawing from the existing cognitive paradigms typical of international relations (IR) also seems to be problematic. Don Munton (2011, p. 116) maintains that 'realist theories are not sufficient for understanding international intelligence cooperation or liaison. To understand both actor interdependence and actors' interests we need to complement realist theory with the perspectives offered by liberal institutionalism and the constructivist approach.' I believe, however, that mid-range cognitive and explanatory formulas provided by mainstream IR theory are insufficient to address the ontological peculiarities of intelligence organisations, and so I examine network theories.

Network science has made impressive advances in recent decades, with researchers and practitioners constantly underlining 'netting', connectivity and clustering (Arquilla and Ronfeldt 2001; Barabási 2002, 2012; Watts 2003). Its intrusion into numerous scientific disciplines has generally been welcomed as it offers an attractive, cohesive and suggestive explanatory framework. Network theories are comprehensive sense-making epistemological constructs addressing one of the basic features of reality: its structural interconnectedness. As Albert-László Barabási (2002, p. 7) wrote in his seminal book: 'Networks are present everywhere. All we need is an eye for them.' Ted Lewis (2009, p. 6) claimed that network science is made up of two key ingredients: the structure of a collection of nodes and links and the dynamic behaviour of the aggregation of nodes and links. Network science allows us to correlate form with function and structure with behaviour. Network theories enable a better understanding of networks as components in various complex systems (Barabási 2012, p. 15). They not only explain the origins and formation of complex systems but most of all address their structure and property as well as architecture and dynamics.

Organisational network structure is composed of nodes which are responsible for the internal behaviour and connectivity of actors (Changizi and He 2005, pp. 13–14). Park and Barabási (2007, p. 17916) observed that 'node properties are not distributed at random in the network, but are correlated with the underlying network structure'. Perreira and others (2013, pp. 1–2) add that networks tend to the synchronisation of diffused elements, reaching a high level of coherence in order to control the behaviour of the nodes. Some nodes have more connections and links connecting to a node are unevenly distributed although they tend to cluster. Such high-level nodes are called hubs and are critical for interconnectedness within multiple dimensions of a network (Berlingerio et al. 2011, pp. 223–5). They shorten the paths between all the nodes in the entire network.

Barabási and Albert (1999, p. 510) identified hubs as a property of free-scale networks. They observed that 'network continuously expands by the addition of new vertices that are connected to the vertices already present in the system'. Hubs are critical for network stability and internal communication between actors. According to Whelan (2012, p. 32), referring to Provan and Kenis's (2007) seminal ideas on network governance, hubs emerge in brokered network governance settings in which activities are controlled by a lead organisation (Shearing and Wood 2000; Dupont 2004; Crawford 2006).

In this book I subscribe to network analysis for ontological as well as methodological reasons. Network analysis of intelligence cooperation highlights complex organisational structure and dense communication systems. From the institutionalist perspective, it properly underlines the relevance of isomorphism as the essential trait of complex organisations acting in heterogeneous environments (Brandes et al. 2013, p. 4).[1] From the functionalist point of view, it demonstrates convincingly the logic of reciprocity and the value of synergetic links between the core elements of a network: nodes and hubs. This is particularly important for intelligence networks built by actors with different levels of competence, tradecraft, security clearance and accountability (den Boer et al. 2008). As early as 1998, Castells wrote that 'A network, by definition, has nodes, not a centre. Nodes may be of different sizes, and may be linked by asymmetrical relationships in the network, so that the network state does not preclude the existence of political inequalities among its members.' (Castells 1998, p. 332).[2]

Nodes and hubs stimulate a host of horizontal and vertical connections that are closely interlinked and exposed to intensive feedback. As far as information networks are concerned, nodes constitute a critical element of a network whereby flows of information, decisions and outcomes are managed, filtered or processed. The nodal model of governance offers a valuable theoretical insight into the structure and dynamics of networked relationships (Shearing and Wood 2003; Burris et al. 2005; Johnston 2006). According to Burris (2004, p. 341), 'The theory of nodal governance is intended to enrich network theory by focusing attention on and bringing more clarity to the internal characteristics of nodes and thus to the analysis of how power is actually created and exercised within a social system. While power is transmitted across networks, the actual point where knowledge and capacity are mobilized for transmission is the node.'

The nodal model is particularly suitable for complex networks which link varied actors and allow for the exchange of different types of resources. Drahos (2004, pp. 404–5) argued that network resources are often brought together through a 'superstructural' node that brings together actors who represent networks, concentrating resources and technologies for the purpose of achieving an adaptive response to a problem that confronts networked governance.

This remark is particularly telling with regard to intelligence networks (Sparrow 1991, pp. 257–8; Treverton and Gabbard 2008, pp. 47–9). They are highly heterogeneous, resistant to integration, prone to closer coordination, susceptible to technological solutions and devices and compliant to state actors. They tend towards clustering and organisation in hubs. The latter emerge from nodes which collect, stockpile and transmit certain information and intelligence belonging to a selected category. Each category is predetermined by source, clearance, safeguards, quality and purpose. Hence, hubs enable the management of information and data in a premeditated, ordered and goal-oriented way, not excluding at the same time intermediary functions and brokering. They demonstrate that the dense network of interconnected entities bound by nodal links could function not only as a useful tool to maintain top-down information workflow but also as a functional pattern of intelligence cooperation focusing on cross-border, spatial, organisational undertakings and operations bringing about positive results in terms of security policies.

The difficulty of studying intelligence cooperation in the EU, including that on the strategic level, lies in the entangled and ill-defined links between the two basic types of intelligence, military and civilian, which reflect the classic division between the intergovernmental (union) and supranational (community) aspects of European integration. The security policies of the EU overlap this division: the Common Security and Defence Policy (CSDP) relies on the military assets provided exclusively by Member States while EU internal security and border management involve measures and activities carried out by agencies and bodies nested in EU supranational structures. As a result, intelligence output at the EU level is subject, predominantly, to vertical bottom-up flows of information and analytical data selected and pre-processed by national intelligence organisations in response to a ‘need to know’ clearly defined by EU customers. This mechanism is particularly appropriate for defence cooperation, which largely depends on the classified information required to plan, command and control military operations under the CSDP. Intelligence support from EU agencies and bodies is principally built on open sources or finished intelligence supplied by Member States for further processing and analysis by EU entities. In the case of EU internal security cooperation, the information flow is much more intensive and diversified. It encompasses various categories of data and a wide range of issues referring to the internal security of EU countries as well as global risks and transnational threats. Horizontal links play a much more important role. They enable an intensive flow of data loaded by relevant national providers and then their collation, comparison and checking against a huge amount of information materials available from an enormous variety of open sources.

This brings us to the final methodological statement. The model of intelligence hubs embedded in a complex networked organisational structure is applied to the analysis of strategic intelligence cooperation in the European Union on the following assumptions:

1. Intelligence hubs emerge on different levels depending on the strength of ties established by the principal actors. They correspond to the main areas of security policies in both national and transnational domains including military, crisis-management, law-enforcement and diplomatic issues.
2. Patterns of isomorphism observable among state actors (at Member-State level) tend to weaken ties, limit network agility and reduce information flow and intelligence sharing. As a result, ‘soft’ hubs are established reflecting the stance of the leading national agency as well as hesitance towards sensitive ‘nationally securitised’ intelligence sharing.
3. The community model is suitable for intelligence cooperation focusing on cross-border phenomena that are seen as the costs of supranational integration, such as transnational criminality or the proliferation of terrorist networks. ‘Hard’ hubs are formed by national law-enforcement authorities willing to share sensitive information with a view to the potential value added by EU institutions and agencies in the course of the collection, analysis and fusion of dispersed data.
4. The EU’s single legal and institutional framework enables synergetic connections and working linkages between horizontally and verti-

> cally oriented intelligence hubs. Intelligence security in the European Union is subject to the ability of all stakeholders—governments of the Member States, local law-enforcement authorities and the military, as well as relevant EU institutions, agencies and bodies—to share their assets, deliver their inputs and use joint intelligence products to strengthen security and public order.

Data for the present book was collected using a combination of desk research and personal interviews with senior officials from the EU, NATO and national authorities as well as leading intelligence experts and scholars conducting research in EU security and intelligence. Individual semi-structured interviews with 14 senior officials were carried out during field trips in June, September and November 2012. Occasional contacts were maintained as a follow-up. The majority of respondents represented EU institutions and agencies: the European Commission (DG Home), the European External Action Service (EU Military Staff, EU Intelligence Analysis Centre), EU Satellite Centre, Europol, Frontex, and the Office of the EU Counter-terrorism Coordinator. NATO's Emerging Security Challenges Division and several national authorities were also represented. All officials agreed to be interviewed only on the condition of strict confidentially. Therefore in the present book any reference to their opinions and statements is anonymised and their exact institutional affiliation is concealed. These discreet encounters were complemented by interviews and talks with 30 experts and scholars from the United Kingdom, the Netherlands, Germany, Spain, Sweden, Denmark, Poland and the Czech Republic.

Plan of the Book

The book is structured around the concept of intelligence hubs. The first two chapters address theoretical, definitional and conceptual aspects of intelligence. The first chapter introduces the concept of intelligence and elaborates on its meaning, theoretical foundations, explanatory properties and cognitive values. The meaning of strategic intelligence is also explained. The concept of the 'intelligence community' is then presented and further discussed with reference to the related terms 'security community' and 'epistemic community'. Considerable differences in the understanding of 'intelligence community' among EU officials and government representatives are explained by the interpretation of the EU intelligence community as a distorted epistemic community.

The next chapter focuses on ‘intelligence tradecraft’ in the EU, that is, the means adopted by stakeholders in the EU intelligence community, the products they offer to EU Member States and the feedbacks to be expected from EU agencies and bodies involved in intelligence sharing. The chapter reflects on the relevance of secrecy and openness in today’s intelligence analysis and contributes to the unfolding debate on the value of open-source information and secret information obtained by national intelligence and counter-intelligence agencies. It also highlights the selective presence of the main intelligence disciplines at the strategic level of EU intelligence cooperation. By the same token the intelligence cycle inherent in strategic analysis of the military aspects of security is juxtaposed with the policy cycle applied in the realm of internal security and criminal intelligence. The final part of the chapter assesses EU intelligence tradecraft to capture the horizontal and vertical determinants stemming from the range of interactions between national and supranational actors. It also offers some explanation of the quintessence of EU intelligence cooperation in technical and organisational terms.

Chapter 4, on military intelligence in the EU, illustrates the predominance of vertical cooperation among Member States, driven by their doctrines and strategies of national security. The problem of defence by military means and support for operations ‘out of EU area’ is tackled in the context of the deficit of political will on the part of individual EU Member States and the political ambitions of the Commission and the High Representative for FASP to gain for the Union the position of a global power. The political endorsement for the concept of a Common Security and Defence Policy led to the creation and progressive expansion of certain institutional arrangements addressing military intelligence cooperation at the EU level. The establishment of the Intelligence Division within the EU Military Staff and the formation of the Joint Situation Centre and the EU Satellite Centre to support military tasks corresponding to missions and operations conducted by EU forces (Petersberg tasks) created intelligence capabilities serving both EU and national interests and objectives.

Chapter 5 is devoted to crisis management in the EU and the role of situational awareness and early warning. The growing importance of the prevention of various threats to EU security and the constant development of crisis-management capabilities is highlighted in the context of information gathering and processing and intelligence sharing. Mechanisms of crisis preparedness and resilience contained in the Crisis

Management Procedures are considered in the context of the need to process and verify the large flow of information and data to appropriate EU agencies, such as the Situation Room and Watch-Keeping Capability. Next, the EU Crisis Response System is examined in the light of institutional capabilities to translate intelligence into effective decisions and actions. In the final part of the chapter, the EU's forecast-analysis and scenario-planning capabilities are evaluated in terms of effective risk management and threat assessment.

EU foreign policy and external relations constitute another dimension of the EU intelligence community. Chapter 6 explains the relevance of socio-cultural intelligence in the EU for the external dimension of EU activities. The political-diplomatic hub established within EEAS contains various mechanisms, instruments and capabilities for gathering and analysing information and data relating to the monitoring of areas outside the Union where risks and threats to EU interests and values may emerge and proliferate. Knowledge of cultural, religious, normative, organisational and political factors seems to be a precondition of the broad scanning of the external environment that is required for a wider view of international security. The role of EEAS is analysed in the context of the surveillance and assessment of the external environment of the Union. The input from Member States is also evaluated and the role of the COREU network is highlighted, given the increasingly binding obligation of Member States to inform and consult each other in matters of foreign affairs and security.

The next chapter takes up the issue of criminal intelligence in the EU. Internal security is a vast area of European integration and it has an increasingly significant impact on the overall security policies of the EU. This chapter examines the organisation, resources, skills, capabilities and results of criminal intelligence in the Union. EU agencies, mostly Europol, Eurojust and Frontex, are assessed in terms of their involvement and input in criminal information exchange, analysis and intelligence sharing. A European Criminal Intelligence Model, the EU policy cycle for organised and serious international crime, and the principles of intelligence-led policing and criminal information management are evaluated as novel approaches to internal security that can make use of communication technologies, large-scale EU-wide IT systems, forensic computer programmes and enhanced analytical capabilities.

The EU intelligence community has been emerging in a global context constructed of transnational threats, external pressures and global risks as well as certain prospects, opportunities and benefits derived from emerging or enhanced patterns of international intelligence cooperation. Chapter 8 describes the partnerships, collaborative efforts and tactical deals made by the EU with actors in the international arena, principally states but also international organisations. The emphasis is on NATO and the United States as strategic partners in security policy.

Chapter 9 identifies and analyses synergetic mechanisms emerging in the institutional, political and strategic realms, and determining the process of formal and informal arrangements, strategic planning, decision making and enforcement. A multi-variant exercise is performed in the central part of this chapter to test the viability of hypotheses formulated at the outset, especially the effect of interactions among particular intelligence hubs which function in permeable and intersecting security fields. The concept of fusion centres is discussed as a practical exemplification of synergy building among diverse intelligence stakeholders. In the final part, a map of intelligence synergies in the EU is presented and explained. It draws on a comprehensive approach to intelligence in the EU and functional relationships between institutional entities concentrated in the hubs. Complex network architecture is tested with reference to interactions, connections, dependencies and feedbacks among the hubs.

Chapter 10 draws attention to the issue of democratic oversight of the EU intelligence community. Although this community does not possess autonomous operational capabilities, it manages the bulk of information discreetly provided by Member States, contributes to the transfer of sensitive data and handles a wide variety of intelligence deliverables. Given the specific nature of EU intelligence cooperation, this chapter elaborates on the concept of tri-dimensional accountability. It underscores the peculiar aspects of intelligence cooperation in the EU by analysing oversight and control functions performed by EU institutions and bodies in two dimensions: the horizontal and the vertical. It also frames the complexity of EU intelligence control mechanisms in the context of tensions between national scrutiny and supranational oversight, largely in relation to the observation that institutional oversight includes a set of measures, procedures and mechanisms generated at the intersection of separate ambits of intelligence management and tradecraft practised in the EU by its agencies and Member States.

The concluding chapter offers some final remarks and suggestions regarding the role of intelligence cooperation in pursuit of a vision of an effective EU security strategy. It makes an overall assessment of the EU intelligence community as a cooperative network encompassing EU institutions, agencies and bodies as well as the competent authorities and services of Member States. The chapter points to the enhanced capacity to deliver and share as well as reduced opportunities to restrict access to information and intelligence relevant to EU security policy objectives, and highlights specific features of the EU intelligence community as a complex network of agencies and practices dedicated to securing strategic EU interests while respecting sensitive national interests due to the reliance of those agencies on Member States' intelligence contributions. Applying a 'hunters and gatherers' metaphor, it discusses the barriers to the establishment of a single EU intelligence agency, and concludes with the thesis that the complex network of institutions, agencies and services involved in the gathering, processing, analysis and exchange of intelligence conducted by Member States within the framework of EU law and strategic agreements constitutes a solid foundation for the EU intelligence community. It fits the model of a phronetic community and is still in the making. As a result, it has displayed numerous shortcomings, systemic deficiencies and distortions. Nevertheless, it makes a remarkable contribution to EU security policies and it strengthens the preventive capabilities of EU agencies and national authorities to cope effectively with the most serious threats and risks.

Notes

1. I present the isomorphic approach to the institutional design of the EU intelligence community in a monograph, *The European intelligence community. Law—institutions—mechanisms* published in Polish by the Jagiellonian University Press (see Gruszczak 2014).
2. However, Barabási (2002, pp. 30–35) seems to take a rather different position.

Bibliography

Agrell, W., & Treverton, G. F. (2015). *National intelligence and science. Beyond the great divide in analysis and policy*. Oxford/New York: Oxford University Press.

Aid, M. W., & Wiebes, C. (Eds.). (2001). *Secrets of signals intelligence during the Cold War and beyond*. London: Frank Cass.

Aldrich, R. J. (1995). European integration: An American intelligence connection. In A. Deighton (Ed.), *Building postwar Europe: National decision makers and European institutions* (pp. 1948–1963). Basingstoke: Macmillan.

Aldrich, R. J. (1998). British intelligence and the Anglo-American 'special relationship' during the Cold War. *Review of International Studies, 24*(3), 331–351.

Aldrich, R. J. (2011). Global intelligence co-operation versus accountability: New facets to an old problem. In L. Scott, R. G. Hughes, & M. S. Alexander (Eds.), *Intelligence and international security. New perspectives and agendas.* London/New York: Routledge.

Alexander, M. S. (1998). Knowing your friends, assessing your allies—Perspectives on intra-alliance intelligence. *Intelligence and National Security, 13*(1), 1–17.

Ansell, C. (2000). The networked polity: Regional development in Western Union. *Governance: An International Journal of Policy and Administration, 13*(4), 303–333.

Argomaniz, J., Bures, O., & Kaunert, C. (2015). A decade of EU counter-terrorism and intelligence: A critical assessment. *Intelligence and National Security, 30*(2-3), 191–206.

Arquilla, J., & Ronfeldt, D. (Eds.). (2001). *Networks and netwars: The future of terror, crime and militancy*. Santa Monica: RAND Corporation.

Baker, C. (2010). *The search for a European intelligence policy*. At http://www.fas.org/irp/eprint/baker.html. Accessed 16 Nov 2011.

Balzacq, Th., & Léonard, S. (2013). Information-sharing and the EU counter-terrorism policy: A 'securitisation tool' approach. In Ch. Kaunert & S. Leonard (Eds.), *European security, terrorism and intelligence: Tackling new security challenges in Europe*. Basingstoke/New York: Palgrave Macmillan.

Bamford, J. (1982). *The puzzle palace: America's National Security Agency and its special relationship with Britain's GCHQ*. London: Sidgwick & Jackson.

Barabási, A.-L. (2002). *Linked. The new science of networks.* Cambridge: Perseus Publishing.

Barabási, A.-L. (2012). The network takeover. *Nature Physics, 8*(1), 14–16.

Barabási, A.-L., & Albert, R. (1999). Emergence of Scaling in Random Networks. *Science, 286,* 509–12.

Berkowitz, B. (1997). Information technology and intelligence reform. *Orbis, 41*(1), 107–118.

Berkowitz, B. D., & Goodman, A. E. (1989). *Strategic intelligence for American national security*. Princeton: Princeton University Press.

Berlingerio, M., et al. (2011). The pursuit of hubbiness: Analysis of hubs in large multidimensional networks. *Journal of Computational Science, 2*(3), 223–237.

Betts, R.K. (2007). *Enemies of intelligence: knowledge and power in American national security.* New York/Chichester: Columbia University Press.

Bigo, D. (1995). Les Etats face aux flux transfrontières de personne: enjeux et perspectives. *Les cahiers de la sécurité intérieure, 19,* 115–125.

Boatner, H. L. (2000). Sharing and using intelligence in international organizations: Some guidelines. *National Security and the Future, 1*(1), 81–92.

Boin, A., Ekengren, M., & Rhinard, M. (2014). *Making sense of sense-making: The EU's role in collecting, analysing, and disseminating information in times of crisis*. Stockholm: Swedish National Defence College.

Bonnefoi, S. (1994). *Europe et sécurité intérieure. TREVI—Union Européenne—Schengen*. Paris: Delmas.

Born, H., & Caparini, M. (Eds.). (2007). *Democratic control of intelligence services: Containing rogue elephants*. Aldershot/Burlington: Ashgate.

Born, H., Johnson, L. K., & Leigh, I. (Eds.). (2005). *Who's watching the spies: Establishing intelligence service accountability*. Dulles: Potomac Books.

Brady, H. (2008). Europol and the European criminal intelligence model: A non-state response to organized crime. *Policing, 2*(1), 103–109.

Brady, H. (2009). *Intelligence, emergencies and foreign policy: The EU's role in counter-terrorism*. London: Centre for European Reform.

Brandes, U., et al. (2013). What is network science? *Network Science, 1*(1), 1–15.

Burris, S. (2004). Governance, microgovernance and health. *Temple Law Review, 77*(2), 335–361.

Burris, S., Drahos, P., & Shearing, C. (2005). Nodal governance. *Australian Journal of Legal Philosophy, 30*(1), 30–58.

Castagna, M. J. (1997). Virtual intelligence: Reengineering doctrine for the information age. *International Journal of Intelligence and CounterIntelligence, 10*(2), 180–195.

Castells, M. (1998). *End of millennium (The information age: Economy, society and culture, vol. III)*. Malden/Oxford: Blackwell Publishers.

Castells, M. (2000). *End of millennium* (2nd ed.). Malden/Oxford: Blackwell Publishers.

Changizi, M. A., & He, D. (2005). Four correlates of complex behavioral networks: Differentiation, behavior, connectivity, and compartmentalization. Carving networks at their joints. *Complexity, 10*(6), 13–40.

Christou, G., et al. (2010). European Union security governance: Putting the 'security' back in. *European Security, 19*(3), 341–359.

Chryssochoou, D. N. (2009). *Theorizing European integration* (2nd ed.). Abingdon/New York: Routledge.

Cini, M. (2006). The 'state of the art' in EU studies: From politics to interdisciplinarity (and back again?). *Politics, 26*(1), 38–46.

Clerix, K. (2014). Ilkka Salmi, the EU's spymaster. *Mondiaal Nieuws*, 4 March. At http://www.mo.be/en/interview/ilkka-salmi-eu-s-007. Accessed 10 June 2014.

Codevilla, A. (1992). *Informing statecraft: Intelligence for a new century*. New York: The Free Press.

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

Coosemans, Th. (2004). *L'Union Européenne et le renseignment: Perspectives de coopération entre les états membres*. Rapport du GRIP 3. Bruxelles: Groupe de recherche et d'information sur la paix et la sécurité.

Cordell, G. (2010). Europe's police information exchange: An exercise in information management. *Journal of Police Studies, 16*, 115–119.

Council of the EU (1995). La Gomera declaration. At http://www.europarl.europa.eu/summits/mad2_en.htm#annex3. Accessed 17 Feb 2009.

Council of the EU (2006c, December 29). Council framework decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. *Official Journal of the European Union, L 386.*

Crawford, A. (2006). Networked governance and the post-regulatory state? Steering, rowing and anchoring the provision of policing and security. *Theoretical Criminology, 10*(4), 449–479.

Dahl, E. J. (2013). *Intelligence and surprise attack: Failure and success from Pearl Harbor to 9/11 and beyond*. Washington, DC: Georgetown University Press.

Davis Cross, M. K. (2011). *Security integration in Europe. How knowledge-based networks are transforming the European Union*. Ann Arbor: The University of Michigan Press.

Davis Cross, M. K. (2013a). Rethinking epistemic communities twenty years later. *Review of International Studies, 39*(1), 137–160.

Davis Cross, M. K. (2013b). The military dimension of European Security: An epistemic community approach. *Millennium – Journal of International Studies, 42*(1), 45–64.

De Jong, T., & Fergusson-Hessler, M. G. M. (1996). Types and qualities of knowledge. *Educational Psychologist, 31*(2), 105–113.

De Jong, B., Platje, W., & Steele, R. D. (Eds.). (2003). *Peacekeeping intelligence—Emerging concepts for the future*. Oakton, VA: OSS International Press.

Den Boer, M. (2002). Intelligence exchange and the control of organized crime: From Europeanisation via centralisation to dehydration? In M. Anderson & J. Apap (Eds.), *Police and justice co-operation and the new European borders.* The Hague/London/New York: Kluwer Law International.

Den Boer, M. (2014). Intelligence-led policing in Europe: Lingering between idea and implementation. In I. Duyvesteyn, B. de Jong, & J. van Reijn (Eds.), *The future of intelligence—Challenges in the 21st century*. Abingdon/New York: Routledge.

Den Boer, M. (2015). Counter-terrorism, security and intelligence in the EU: Governance challenges for collection, exchange and analysis. *Intelligence and National Security, 30*(2-3), 402–419.

Den Boer, M., Hillebrand, C., & Nölke, A. (2008). Legitimacy under pressure: The European web of counter-terrorism networks. *Journal of Common Market Studies, 46*(1), 101–124.

Díaz Fernández, A., Revenga Sánchez, M., & Jiménez, O. J. (2009). *Cooperación Europea en Inteligencia: nuevas preguntas, nuevas respuestas.* Ed. Aranzadi: Pamplona.

Donath, J. (1993). A European Community Intelligence Organization. *Defense Intelligence Journal, 2*(1), 15–33.

Dorn, A. W. (1999). The cloak and the blue beret: Limitations on intelligence in UN peacekeeping. *International Journal of Intelligence and Counterintelligence, 12*(4), 414–447.

Dorn, N. (2008). European strategic intelligence: How far integration? *Erasmus Law Review, 1*(5), 163–180.

Dorn, A. W. (2010). United Nations peacekeeping intelligence. In L. K. Johnson (Ed.), *The Oxford handbook of national security intelligence.* Oxford: Oxford University Press.

Drahos, P. (2004). Intellectual property and pharmaceutical markets: A nodal governance approach. *Temple Law Review, 77*(2), 401–424.

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

Dupont, B. (2004). Security in the age of networks. *Policing and Society, 14*(1), 76–91.

Duyvesteyn, I., de Jong, B., & van Reijn, J. (Eds.). (2014). *The future of intelligence. Challenges in the 21st century.* Abingdon/New York: Routledge.

Egan, M., Nugent, N., & Paterson, W. E. (Eds.). (2010). *Research agendas in EU studies. Stalking the elephant.* Basingstoke/New York: Palgrave Macmillan.

Ehrhart, H.-G., Hegemann, H., & Kahl, M. (2014a). Towards security governance as a critical tool: A conceptual outline. *European Security, 23*(2), 145–162.

European Union (2012). Treaty on European Union (consolidated version). *Official Journal of the European Union*, C 326, 26 October.

Fägersten, B. (2008). *European intelligence cooperation: Drivers, interests and institutions.* SIIA Papers, br. 6. Stockholm: The Swedish Institute of International Affairs.

Fägersten, B. (2010). Bureaucratic resistance to international intelligence cooperation—The case of Europol. *Intelligence and National Security, 25*(4), 500–520.

Fägersten, B. (2014). European intelligence cooperation. In I. Duyvesteyn, B. de Jong, & J. van Reijn (Eds.), *The future of intelligence—Challenges in the 21st century.* Abingdon/New York: Routledge.

Ferris, J. (2004). Netcentric warfare, C4ISR and information operations: Towards a revolution in military intelligence? *Intelligence and National Security, 19*(2), 199–225.

Fingar, T. (2011). *Reducing uncertainty: Intelligence analysis and national security*. Stanford: Stanford University Press.

Fisher, R., & Johnston, R. (2008). Is intelligence analysis a discipline? In R. Z. George & J. B. Bruce (Eds.), *Analyzing intelligence: Origins, obstacles, and innovations*. Washington, DC: Georgetown University Press.

Freedman, L. (1986). *US intelligence and the Soviet threat* (2nd ed.). Princeton: Princeton University Press.

Gariup, M. (2009). *European security culture: Language, theory, policy*. Farnham/ Burlington: Ashgate.

Gill, P. (2006). Not just joining the dots but crossing the borders and bridging the voids: Constructing security networks after 11 September 2001. *Policing & Society, 16*(1), 27–49.

Gill, P., & Phythian, M. (2006). *Intelligence in an insecure world*. Cambridge: Polity Press.

Gill, P., Marrin, S., & Phythian, M. (Eds.). (2009). *Intelligence theory. Key questions and debates*. Abingdon/New York: Routledge.

Giumelli, F., & Lavallée, C. (2013). EU security governance: From processes to policies. *Journal of Contemporary European Research, 9*(3), 365–371.

Grenfell, D., & James, P. (2009). Debating insecurity in a globalizing world. An introduction. In D. Grenfell & P. James (Eds.), *Rethinking insecurity, war and violence. Beyond savage globalization?* Abingdon/New York: Routledge.

Gries, D. D. (1991). Intelligence in the 1990s. *Studies in Intelligence, 35*, 5–12.

Gruszczak, A. (2013). EU intelligence-led policing: The case of counter-terrorism cooperation. In M. O'Neill, K. Swinton, & A. Winter (Eds.), *New challenges for the EU internal security strategy*. Newcastle upon Tyne: Cambridge Scholars Publishing.

Gruszczak, A. (2014). *Europejska wspólnota wywiadowcza. Prawo—instytucje—mechanizmy*. Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego.

Hager, N. (1996). *Secret power*. Nelson: Craig Potton Publishing.

Hajer, M., & Versteek, W. (2005). Performing governance through networks. *European Political Science, 4*(3), 340–347.

Hebenton, B., & Thomas, T. (1995). *Policing Europe*. London: Macmillan Press.

Herman, M. (1996). *Intelligence power in peace and war*. Cambridge: Cambridge University Press.

Hertzberger, E. R. (2007). *Counter-terrorism intelligence cooperation in the European Union*. Turin: UNICRI.

Hoffman, B. (1996). Intelligence and terrorism: Emerging threats and new security challenges in the post-Cold War era. *Intelligence and National Security, 11*(2), 207–223.

Hollis, S. (2010). The necessity of protection: Transgovernmental networks and EU security governance. *Cooperation and Conflict, 45*(3), 312–330.

Honig, O. A. (2007). A new direction for theory-building in intelligence studies. *International Journal of Intelligence and CounterIntelligence, 20*(4), 699–716.

Hulnick, A.S. (1991–2). Intelligence cooperation in the post-Cold War era: A new game plan?. *International Journal of Intelligence and CounterIntelligence*, 5(4), 455–465.

Hulnick, A. S. (2006b). U.S. intelligence reform: Problems and prospects. *International Journal of Intelligence and CounterIntelligence, 19*(2), 302–315.

Ingram, A., & Dodds, K. (2009). Spaces of security and insecurity: Geographies of the war on terror. In A. Ingram & K. Dodds (Eds.), *Spaces of security and insecurity: Geographies of the War on Terror*. Farnham/Burlington: Ashgate.

Jackson, P., & Siegel, J. (2005). Introduction. In P. Jackson & J. Siegel (Eds.), *Intelligence and statecraft. The use and limits of intelligence in international society*. Westport/London: Praeger.

Jäger, T., & Daun, A. (2009). Intelligence in der EU. Restriktionen und Handlungsmöglichkeiten von Agenten und Prinzipalen. In T. Jäger & A. Daun (Eds.), *Geheimdienste in Europa: Transformation, Kooperation und Kontrolle*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Jeffreys-Jones, R. (2007). The idea of a European FBI. In L. K. Johnson (Ed.), *Strategic intelligence* (Vol. 4). Westport/London: Praeger Security International.

Jeffreys-Jones, R. (2009). Rise, fall and regeneration: From CIA to EU. *Intelligence and National Security, 24*(1), 103–118.

Jeffreys-Jones, R. (2011). Rise, fall and regeneration: From CIA to EU. In L. Scott, R. G. Hughes, & M. S. Alexander (Eds.), *Intelligence and international security. New perspectives and agendas*. London/New York: Routledge.

Jervis, R. (2010). *Why intelligence fails: Lessons from the Iranian Revolution and the Iraq War*. Ithaca/London: Cornell University Press.

Johnson, L. K., & Shelton, A. M. (2013). Thoughts on the state of intelligence studies: A survey report. *Intelligence and National Security, 28*(1), 109–120.

Johnston, L. (2006). Transnational security governance. In J. Wood & B. Dupont (Eds.), *Democracy, society and the governance of security*. Cambridge: Cambridge University Press.

Jones, M., & Silberzahn, Ph. (2013). *Constructing Cassandra: Reframing intelligence failure at the CIA, 1947–2001*. Stanford: Stanford University Press.

Kahn, D. (2009). An historical theory of intelligence. In P. Gill, S. Marrin, & M. Phythian (Eds.), *Intelligence theory. Key questions and debates*. Abingdon/New York: Routledge.

Kaunert, Ch., & Léonard, S. (Eds.) (2013). *European security, terrorism and intelligence: Tackling new security challenges in Europe*. Basingstoke/New York: Palgrave Macmillan.

Keast, R. (2014). Network theory tracks and trajectories. Where from, where to? In R. Keast, M. Mandell, & R. Agranoff (Eds.), *Network theory in the public sector. Building new theoretical frameworks*. New York/Abingdon: Routledge.

Kirchner, E. J., & Sperling, J. (2007). *EU security governance*. Manchester: Manchester University Press.

Klerks, P. (1993). *An inventory of European intelligence services.* Amsterdam: Stichting voor Onderzoek naar Binnenlandse Veiligheid. At http://www.blythe.org/Intelligence/readme/Eurointel. Accessed 22 Dec 2012.

Krahmann, E. (2003). Conceptualizing security governance. *Cooperation and Conflict, 38*(5), 5–26.

Kriendler, J. (2006). *NATO Intelligence and Early Warning.* Special Series 06/13. Watchfield: Conflict Studies Research Centre.

Laino, K. (2011). The transformation of the intelligence paradigm in NATO. In S. R. Di Rienzo, D. Crncec, & L. Brozic (Eds.), *Regional security and intelligence cooperation in the Western Balkans and global asymmetric threats.* Ljubljana: Defensor.

Lefebvre, S. (2003). The difficulties and dilemmas of international intelligence cooperation. *International Journal of Intelligence and CounterIntelligence, 16*(4), 527–542.

Lelieveldt, H., & Princen, S. (2011). *The politics of the European Union*. Cambridge: Cambridge University Press.

Lewis, T. G. (2009). *Network science: Theory and practice*. Hoboken: Wiley.

Lorber, A. (2015). *Ready for battle: Technological intelligence on the battlefield.* Lanham/Boulder/New York/London: Rowman & Littlefield.

Mattli, W. (1999). *The logic of regional integration. Europe and beyond*. Cambridge: Cambridge University Press.

Mérand, F., Hofmann, S., & Irondelle, B. (2011). Governance and state power: A network analysis of European security. *Journal of Common Market Studies, 49*(1), 121–147.

Messervy-Whiting, G. (2004). Intelligence cooperation in the European Union. In J. Pilegaard (Ed.), *The politics of European security*. Copenhagen: Danish Institute for International Studies.

Müller-Wille, B. (2002). EU intelligence co-operation. A critical analysis. *Contemporary Security Policy, 23*(2), 61–86.

Müller-Wille, B. (2004). *For our eyes only? Shaping an intelligence community within the EU*. Occasional Papers no. 50. Paris: EU Institute for Security Studies

Müller-Wille, B. (2008). The effect of international terrorism on EU intelligence cooperation. *Journal of Common Market Studies, 46*(1), 49–73.

Munton, D. (2011). Intelligence cooperation meets international studies theory: Explaining Canadian operations in Castro's Cuba. In L. Scott, R. G. Hughes, & M. S. Alexander (Eds.), *Intelligence and international security. New perspectives and agendas.* London/New York: Routledge.

Nomikos, J. (2004). European Union intelligence agency: A necessary institution for common intelligence policy? In V. N. Koutrakou (Ed.), *Contemporary issues* *and debates in EU policy. The European Union and international relations.* Manchester/New York: Manchester University Press.

Nomikos, J. M. (2005). A European Union intelligence service for confronting terrorism. *International Journal of Intelligence and CounterIntelligence, 18*(2), 191–203.

Nutt, K., & Pal, L. A. (2011). "Modernizing government": Mapping global public policy networks. *Governance: An International Journal of Policy, Administration, and Institutions, 24*(3), 439–467.

Park, J., & Barabási, A.-L. (2007). Distribution of node characteristics in complex networks. *PNAS, 104*(46), 17916–17920.

Pereira, T., et al. (2013). Connectivity driven coherence in complex networks. *Physical Review Letters, 110*(23), 1–5.

Phythian, M. (2009). Intelligence theory and theories of international relations. Shared world or separate worlds? In P. Gill, S. Marrin, & M. Phythian (Eds.), *Intelligence theory. Key questions and debates.* Abingdon/New York: Routledge.

Pillar, P. R. (2011). *Intelligence and US foreign policy: Iraq, 9/11, and misguided reform.* New York: Columbia University Press.

Politi, A. (1997). *European security: The new transnational risks.* Chaillot Paper no. 29. Paris: Institute for Security Studies of the WEU.

Politi, A. (Ed.). (1998a). *Towards a European intelligence policy.* Chaillot Paper No. 34. Paris: Institute for Security Studies of the WEU.

Posner, R. A. (2005). *Preventing surprise attacks: Intelligence reform in the wake of 9/11.* Lanham: Rowman & Littlefield.

Prados, J. (1982). *The Soviet estimate: US intelligence analysis and Russian military strength.* New York: The Dial Press.

Provan, K. G., & Kenis, P. (2007). Models of network governance: Structure, management and effectiveness. *Journal of Public Administration Research and Theory, 18*(2), 229–252.

Reveron, D. (2006). Old allies, new friends: Intelligence-sharing in the war on terror. *Orbis, 50*(3), 453–468.

Reynolds, D. (1985/6). A "special relationship"? America, Britain and the international order since the Second World War. *International Affairs*, 62(1), 1–20.

Ricci, A. (2008). Introduction. In A. Ricci (Ed.), *From early warning to early action? The debate on the enhancement of the EU's crisis response capability continues.* Luxembourg: Office for Official Publications of the European Communities.

Richelson, J. (1985). *The U.S. intelligence community.* New York: Ballinger.

Richelson, J. (1986). *Sword and shield: The Soviet intelligence and security apparatus.* New York: Ballinger.

Richelson, J. T. (1990). The calculus of intelligence cooperation. *International Journal of Intelligence and CounterIntelligence, 4*(3), 307–323.

Richelson, J. T. (1996). High flyin' spies. *The Bulletin of the Atomic Scientists, 52*(5), 48–54.

Richelson, J. T., & Ball, D. (1985). *The ties that bind: Intelligence cooperation between the UKUSA countries, the United Kingdom, the United States of America, Canada, Australia, and New Zealand*. New York: Allen and Unwin.

Robertson, K. (1994). Practical police co-operation in Europe: The intelligence dimension. In M. Anderson & M. den Boer (Eds.), *Policing across national boundaries.* London: Pinter.

Rosamond, B. (2000). *Theories of European integration*. New York: St. Martin's Press.

Rovner, J., & Long, A. (2005–6). The perils of shallow theory: Intelligence reform and the 9/11 commission. *International Journal of Intelligence and CounterIntelligence, 18*(4), 609–637.

Rüter, J. (2007). *European external intelligence co-operation*. Saarbrücken: VDM Verlag Dr. Müller.

Scharpf, F. (1994). Games real actors could play: Positive and negative coordination in embedded negotiations. *Journal of Theoretical Politics, 6*(1), 27–53.

Scott, L., & Hughes, R. G. (2011). The future of intelligence: Seeking perfection in an imperfect world? In L. Scott, R. G. Hughes, & M. S. Alexander (Eds.), *Intelligence and International Security. New Perspectives and Agendas.* London/New York: Routledge.

Scott, L., & Jackson, P. (2004). Journeys in shadows. In P. Jackson & L. V. Scott (Eds.), *Understanding intelligence in the twenty-first century. Journeys in shadows.* London/New York: Routledge.

SDA (2011, September 22). The need to know: European information-sharing. SDA roundtable report. At http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/2907/The-need-to-know-European-informationsharing.aspx. Accessed 7 Mar 2013.

Shapcott, W. (2011). Do they listen? Communicating warnings: An intelligence practitioner's perspective. In Ch. de Franco & Ch. O. Meyer (Eds.), *Forecasting, warning, and responding to transnational risks.* Basingstoke/New York: Palgrave Macmillan.

Shearing, C., & Wood, J. (2000). Reflections on the governance of security: A normative enquiry. *Police Practice: An International Journal, 1*(4), 457–476.

Shearing, C., & Wood, J. (2003). Nodal governance, democracy, and the new 'denizens'. *Journal of Law and Society, 30*(3), 400–419.

Sims, J. E. (2006). Foreign intelligence liaison: Devils, deals, and details. *International Journal of Intelligence and CounterIntelligence, 19*(2), 195–217.

Smith, H. (1994). Intelligence and UN peacekeeping. *Survival, 36*(3), 174–192.

Sparrow, M. K. (1991). Network vulnerabilities and strategic intelligence in law enforcement. *International Journal of Intelligence and CounterIntelligence, 5*(3), 255–274.

Staab, A. (2011). *The European Union explained: Institutions, actors, global impact.* Bloomington: Indiana University Press.

Steele, R. D. (1995). Private enterprise intelligence: Its potential contribution to national security. *Intelligence and National Security, 10*(4), 212–228.

Steele, R. D. (2006). Peacekeeping intelligence and information peacekeeping. *International Journal of Intelligence and CounterIntelligence, 19*(3), 519–537.

Svendsen, A. D. M. (2008a). The globalization of intelligence since 9/11: Frameworks and operational parameters. *Cambridge Review of International Affairs, 21*(1), 129–144.

Svendsen, A. D. M. (2008b). The globalization of intelligence since 9/11: The optimization of intelligence liaison arrangements. *International Journal of Intelligence and CounterIntelligence, 21*(4), 661–678.

Svendsen, A. D. M. (2010). *Intelligence cooperation and the war on terror. Anglo-American security relations after 9/11.* Abingdon/New York: Routledge.

Svendsen, A. D. M. (2011). On 'a continuum with expansion'? Intelligence co-operation in Europe in the early twenty-first century. *Journal of Contemporary European Research, 7*(4), 520–538.

Torfing, J. (2005). Governance network theory: Towards a second generation. *European Political Science, 4*(3), 305–315.

Treverton, G.F. (1995). *The intelligence agenda*. RAND Paper P-7941. Santa Monica: RAND.

Treverton, G. F., & Gabbard, C. B. (2008). *Assessing the tradecraft of intelligence analysis.* RAND Technical Report TR-293. Santa Monica: RAND Corporation.

Turner, M. A. (2005). *Why secret intelligence fails.* Dulles: Potomac Books.

Tuzuner, M. (Ed.). (2010). *Intelligence cooperation practices in the 21st century: Towards culture of sharing*. Amsterdam: IOS Press.

Vaz Antunes, J. N. J. (2005). European Union Military Staff's Intelligence Division. Developing an intelligence capability: The European Union. *Studies in Intelligence, 49*(4), 65–70.

Villadsen, O. R. (2000). Prospects for a european common intelligence policy. *Studies in Intelligence, 44*(9), 81–95.

Walsh, J. I. (2006). Intelligence-sharing in the European Union: Institutions are not enough. *Journal of Common Market Studies, 44*(3), 625–643.

Walsh, J. I. (2007). Defection and hierarchy in international intelligence sharing. *Journal of Public Policy, 27*(2), 151–181.

Warner, M. (2007). Sources and methods for the study of intelligence. In L. K. Johnson (Ed.), *Handbook of intelligence studies.* London/New York: Routledge.

Watts, D. J. (2003). *Six degrees. The science of a connected age*. New York/London: W.W. Norton & Company.

Watts, D. (2008). *The European Union*. Edinburgh: Edinburgh University Press.

Webber, M., et al. (2004). The governance of European security. *Review of International Studies, 30*(1), 3–26.

Wetzling, T. (2008). European counterterrorism intelligence liaisons. In S. Farson, P. Gill, M. Pythian, & S. Shpiro (Eds.), *PSI handbook of global security and intelligence: National approaches* (Vol. 2). Westport: Praeger.

WEU (1995a, November 14). *European Security: A Common Concept of the 27 WEU Countries.* Extraordinary Council of Ministers, Madrid. At http://www.bits.de/NRANEU/docs/WEU141195.PDF. Accessed 17 Apr 2012.

Whelan, Ch. (2012). *Networks and national security. Dynamics, effectiveness and organisation*. Farnham/Burlington: Ashgate.

Wiebes, C. (2003). *Intelligence and the war in Bosnia, 1992–1995.* New Brunswick: Transactions Publishers.

Wirtz, J. J. (2007). The American approach to intelligence studies. In L. K. Johnson (Ed.), *Handbook of intelligence studies.* London/New York: Routledge.

Završnik, A. (2013). Blurring the line between law enforcement and intelligence: Sharpening the gaze of surveillance? *Journal of Contemporary European Research, 9*(1), 181–202.

Zegart, A. B. (2005). September 11 and the adaptation failure of US intelligence agencies. *International Security, 29*(4), 78–111.

Zegart, A. B. (2006). An empirical analysis of failed intelligence reforms before September 11. *Political Science Quarterly, 121*(1), 33–60.

CHAPTER 2

The Strategic Intelligence Community

Strategic intelligence is not a topic to fascinate a general public regaled by stories of superspies, brave special agents or vicious hostile services penetrating quiet localities with evidently bad intentions. It is rather a bureaucratised, hierarchic, often boring field of everyday labour consisting in—generally speaking—knowledge management (Waltz 2003, pp. 1–3). In simplistic terms, strategic intelligence deals with information, data and the outcomes of their processing and refining in the pursuit of predictability, reliability and the effectiveness of activities already underway. Such a rational approach to strategic intelligence is typical of thinking about security and 'doing security' (Button 2008) in terms of military, law-enforcement, economic, diplomatic and societal resources. Rationality underpins strategy; this entails systematic calculation, feasible planning, the premeditated application of ways and means, and the responsible supervision of actions taken.[1] According to Harry Yarger, strategy is 'the calculation of objectives, concepts, and resources within acceptable bounds of risk to create more favorable outcomes than might otherwise exist by chance or at the hands of others' (Yarger 2006, p. 1). Strategic intelligence, then, is the purposeful management of knowledge that reveals critical threats and opportunities, serving decision-making needs by comprehensively linking means with ends and mission.

'Strategic intelligence' combines 'strategy' and 'intelligence', although the relationship of the two words is subject to various interpretations

A. Gruszczak, *Intelligence Security in the European Union*,
DOI 10.1057/978-1-137-45512-3_2

(Heuser 2010, pp. 4–7). Strategy, in essence, determines the meaning, forms and practical value of intelligence. Throughout the history of states and nations, intelligence has most often served national security purposes determined by external factors: hostile tribes or nations, competing powers, or political opposition in exile. The task of defending sovereignty and territory against foreign enemies and external threats has usually been mandated to the armed forces and military intelligence. Strategic thought, then, was saturated with the rich tradition of the art of war and military history (Lykke, Jr. 1989; Collins 2002; Jablonsky 2004; Heuser 2010; Blanken 2012; Freedman 2013).

Contemporary security strategy and policy are in constant need of effectively managed intelligence in a security environment that is becoming more turbulent and complex, breeding sources of risk, rivalry and conflict. Strategic intelligence and knowledge sharing have become more sophisticated and more relevant for national and international security due to the following factors:

- the growing number and intensity of threats, crises and conflicts which require a reaction from national and international actors;
- the increasing importance of precautionary approaches to security that focus on preventive, pre-emptive and anticipatory measures;
- the propensity of state actors and international organisations to more collective action and less individual effort when dealing with major crises and vital security dilemmas;
- the need to access advanced technologies and sophisticated tools enabling massive information collecting, processing and disseminating, and knowledge sharing;
- the opportunity for private, non-state or anti-state entities to widely apply intelligence tradecraft. (Xu and Kaye 2007, pp. 36–54).

Strategic intelligence, then, is an outcome of organisational frameworks established to enable the realisation of a general strategy and thereby perform essential functions, promoting interests and effectively managing the resources at the disposal of a collective actor (non-state entity, private company, government, international organisation).

The strategic perspective on intelligence presented in this chapter is a conceptual and definitional exercise intended to highlight the complex nature of intelligence activities in the traditional sense of national security and state policies as well as in the contemporary setting permeated by networks and complex systems intersecting the various levels of security policies and strategies. Therefore, it is important to conceptualise intelligence in an active security environment determined not only by national interests and identities but also by transnational networks underpinning information flows and stimulating intelligence sharing beyond national 'silos'. In this context, an intelligence community is presented as a sort of knowledge-based community network seeking to enhance its analytical capabilities through extended access to the information, knowledge and expertise held by relevant intelligence actors.

What Is Intelligence?

The increasingly broad application of the concept of intelligence has been a significant feature of contemporary intelligence studies. Obviously, it attracts criticism from mainstream intelligence officials and scholars afraid of information overload, declining standards of intelligence activities, the widening margins of error in intelligence analysis, and even potentially devastating effects of these for decision making and democratic governance (Agrell 2002). The fear of the 'digital tsunami' and unintended consequences of global information flows is another 'curse' of today's intelligence. The problem of information reliability, already identified half a century ago as the 'signals and noises' dilemma,[2] nowadays needs a particularly prudent approach given the 'information bomb' detonated by the Internet and the social media revolution (Terranova 2004; Papacharissi 2009; Trottier 2012; White 2012; Gupta and Brooks 2013; Altshuler et al. 2013; Herrera 2014).

A detailed elaboration of the meaning, concepts and definitions of intelligence is definitely beyond the scope and scale of this book. For the sake of clarity, but also with direct reference to the book's conceptual framework, intelligence is here conceived as a politically driven activity situated on the strategic level of decision making in support of the policy process, especially when national security, defence, international relations and global issues are at stake. Setting intelligence in the strategic context is justified on the grounds that it is considered to be one of the most sensitive areas of state policy and a specific type of activity in the field of national security (Lowenthal 2009, p. 5). Elevating intelligence cooperation to the international level does not substantially change this approach (Lander 2004) because the essence of collaboration remains in the domain of national security while forms of international or cross-border cooperation emerge as isomorphic patterns of domestic intelligence settings.

However, transnational forms and mechanisms may have a significant impact on national intelligence structures when sufficient synergy effects are produced by contributing national units. These effects should be experienced in decision-making processes and utilised by policy makers for effective management. This is particularly important in the contemporary conditions of uncertainty, information overload, network complexity and bureaucratisation of the intelligence apparatus. Richard K. Betts (2003, p. 59; also Jeffreys-Jones 2011, pp. 98–9) grasped this idea in the following statement: 'To be useful, intelligence analysis must engage policymakers' concerns. Policy-makers who utilize analysis need studies that *relate* to the objectives they are trying to achieve. Thus analysis must be sensitive to the policy context, and the range of options available, to be of any use in making policy.'

In many definitions, especially those dating from the Cold War period, intelligence has been identified with information. Vernon Walters, a US Army general, diplomat and once Deputy Director of Central Intelligence (1972–1976), asserted that 'Intelligence is information, not always available in the public domain, relating to the strength, resources, capabilities, and intentions of a foreign country that can affect our lives and the safety of our people' (Walters 1978, p. 621). Walter Laqueur (1985, pp. 11–12), while recognising the complex nature of intelligence, asserted that information is one of the facets of intelligence. Stansfield Turner, a former US Director of Central Intelligence, pointed out in the last years of the Cold War that 'having the best information is the key to success in almost any line of endeavor' (Turner 1991, p. 151). In Warner's view, intelligence is 'a type of privileged information, and the activity of acquiring, producing, and possibly acting on that information' (Warner 2009, p. 16). So, access to intelligence used to be limited to and was often reserved for authorised customers representing top state decision-making bodies.

The collection of available information is deemed absolutely indispensable for running the analytical cycle and obtaining any valuable intelligence product (Betts 2007, pp. 178–82; Kahn 2009, p. 4; Hall and Citrenbaum 2010, pp. 17–20). Apart from lending support to decision-making procedures and processes, intelligence should enhance security through warnings and alerts (Lowenthal 2009, p. 7). Information has been commonly considered a prerequisite of early warning and preparedness and as such has been seen as another strategic resource for effective governance and the maintenance of public order (Hilsman, Jr. 1952, p. 5; Ben-Zvi 1976).

Many scholars and practitioners have observed that intelligence is inextricably linked not only to the concept of information but also to knowledge (Brown 2007, p. 337; Agrell and Treverton 2015). A radical inductionist view presented by Hilsman (1956, pp. 62–4) highlighted the essential links between information ('facts') and knowledge. The lack or deficit of information undermines knowledge production and therefore precludes the development of effective intelligence. However, in the face of the rising tide of information, data and facts, the need for comprehensive, profound and insightful knowledge is especially acute.

Albert Einstein (1954, p. 271) once noted that 'information is not knowledge since knowledge is inextricably linked to experience'. In the contemporary world information is not enough. Knowledge matters. Intelligence is the production of knowledge on the basis of experience. Intelligence activities focus on knowledge as the central resource in the achievement of strategic goals. Andrew Rathmell (2002, pp. 88–9), in his widely discussed article on postmodern intelligence, stressed that 'the business of the intelligence community is the production of knowledge. Not just any knowledge, but targeted, actionable and predictive knowledge for specific consumers. Secret sources and methods will contribute to this process but only as a part of the whole.'

State authorities, public administration, civil society and international organisations expect from intelligence services timely, reliable and useful knowledge of threats and risks to national and international security. They also need to be informed of imminent dangers and natural hazards that could disrupt their routine activities and produce a traumatic breakdown, undermining order, stability and welfare. This aspect of intelligence has accompanied theoretical and conceptual proposals since the beginning of intelligence studies. Sherman Kent, an outstanding US intelligence officer and scholar, often described as 'the father of intelligence analysis', stated that 'Intelligence […] is the knowledge that our highly placed civilians and military men must have to safeguard the national welfare' (Kent 1966, p. vii). He also found that policy makers are not always capable of managing the challenge of optimal decision making and that is why they need intelligence analysts to support them with background knowledge, tradecraft expertise, analytical skills and experience (Kent 1966, pp. 147–8; comp. Kendall 1949, pp. 546–7; Davis 2002, p. 9).

The utility of intelligence was highlighted in the post-9/11 debate when the issue of the practicality and effectiveness of intelligence communities was put high on the agenda. A significant shift from tradecraft as art to tradecraft as practical skills was widely recommended. The post-9/11 conceptualisation of intelligence underscored its practical aspects and utility for policy making and security governance (Dupont 2003; Gill 2004; Phythian 2005; Moore 2007; Treverton 2009; Breakspear 2013). Intelligence, according to Manosevitz (2013, p. 15), helps policy makers to avoid surprise and understand evolving developments, as well as identify opportunities to advance national objectives or avoid risks to national security interests. In a similar vein, Wheaton and Beerbower (2006, p. 329; also Bowman 2012; Clark 2013, pp. 29–30) assert that the aim of intelligence is to reduce the decision maker's level of uncertainty to the minimum possible.

Mark Lowenthal, the author of a well-known monograph on theoretical and practical aspects of intelligence, conceives intelligence as the process 'by which specific types of information important to national security are requested, collected, analyzed, and provided to policy makers' (Lowenthal 2008, p. 19). Though intelligence serves political objectives, it is often politicised and subordinated to decision makers who may lack professional knowledge and skills but are prone to interfering with the intelligence community and manipulating its analytical art and tradecraft (Handel 1987, pp. 6–7; Rovner 2011, pp. 8–13; 2013, pp. 55–6; Woodard 2013, pp. 96–7). In extreme cases, this may produce misinformation and lead to serious intelligence errors (Bamford 2004; Jervis 2006; Dahl 2011; Shelton 2011; Rovner 2011, pp. 142–55).

Gill and Phythian, outstanding scholars in the field of intelligence studies, connect intelligence with security, but see this relationship in a wider perspective. They write: 'Intelligence refers to the range of activities aiming to maintain or enhance security by delivering specific knowledge of threats and risks allowing for a proper reaction or prevention in terms of strategy, policy and action, including covert activities when necessary' (Gill and Phythian 2006, p. 7; 2012, pp. 11–12).

Many intelligence practitioners and scholars have underlined the utmost importance of secrecy. Their position, particularly expressive when confronted with the rising popularity of open-source intelligence and large-scale data processing, is guided by a narrow definition of intelligence as 'secret information obtained by secret means' (Barger 2005, p. 28). They also point to the inherent conflict between secrecy, openness and efficacy (Johnston 2005a, p. xvi; Tucker 2014, pp. 33–5).

The traditional image of a secret agent or a spymaster seems to be increasingly outdated and obsolete these days. The confrontation between an individual and an organisation, a single expert versus large national and international networks, brilliant human cognitive and deductive abilities versus highly sophisticated data-processing machines results more often than not in an individual being disadvantaged. The debate surrounding 'traditional' and 'modern' intelligence addresses, amongst other factors, the issue of secrecy and openness, or the ultimate relevance of open sources and secret or restricted information. The exchange of arguments between supporters and opponents of both orientations is of the utmost importance because it seeks to establish a firm ground for intelligence analysis and studies for the coming years, or even decades. The question is not of the 'either/or' kind, but one that addresses the tendencies in the current intelligence landscape in the context of the political, cultural, societal and technological changes and shifts that we have been witnessing in the last quarter of a century.

It is therefore very important to reflect on the relevance and significance of secrecy in modern intelligence. For Gill and Phythian, secrecy is an indispensable condition of intelligence processes. Their definition of intelligence is the following: 'the mainly secret activities—targeting, collection, analysis, dissemination and action—intended to enhance security and/or maintain power relative to competitors by forewarning of threats and opportunities' (Gill and Phythian 2012, p. 19). Mark Lowenthal (2008, p. 8) asserted in a similar vein that 'The pursuit of secret information is the mainstay of intelligence activity' (comp. Westerfield 1996, 528–45). Certainly, secrecy underpins intelligence and is crucial for a pro-active approach to the most serious threats to national security and public order.[3] Terrorism, organised crime, cyber-attacks and the proliferation of weapons of mass destruction (WMD) take their toll only when they are the final outcome of premeditated, well planned and deeply secretive hidden operations. The clandestine nature of illegal activities is designed to protect their perpetrators against unmasking by state security agencies or law-enforcement services through surveillance, policing and intelligence analysis.

The Internet revolution has led to rapid growth in intelligence services' interest in the information and data resources available through global communication connections. In recent years, cloud computing, big-data warehousing and data-mining applications have given analysts sight of a great deal of sensitive information privately originated, stored in electronic communication networks and used in Web services (Babcock 2010). The growing popularity of open-source intelligence (OSINT) is owing to the relative ease and safety of access to varied sources of data and information (Nicander 2011, pp. 548–9). OSINT focuses on the collection of legally available documents, the monitoring of the political, economic, military and social activities of states, societies and economic actors, and the exploitation of information generated in the public domain by public and social media, commercial entities, and research outlets (governmental and non-governmental research institutes, think tanks and academic institutions) (Richelson 1999, p. 274; Gibson 2004, p. 19; Bean 2011; Olcott 2014, pp. xii–xiii). A special category consists of classified files leaked by 'whistleblowers' such as Manning, Assange or Snowden. The advantages of OSINT were already being highlighted in the post-WWII years by top officials of the nascent US intelligence community. William Donovan, the 'father of American intelligence', tasked by President Roosevelt to establish a US intelligence service, was at first totally committed to the idea that 'by searching through the Library of Congress and through the files of the many government agencies [scholars] could uncover much of the information for which secret agents risked their lives' (Hilsman, Jr. 1952, p. 1). Former officers of the US intelligence services acknowledged that open sources are the 'basic building blocks' of secret intelligence (Hulnick 1999, pp. 40–1; Mercado 2004). Leaving aside the arguments put forward by followers and opponents of open-source intelligence, one can quote Lord Dacre's apt phrase: 'Secret intelligence is the continuation of open intelligence by other means.'[4]

The Intelligence Cycle

Any intelligence tradecraft is subject to a model of sequential activities allowing for the systematic, 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 the quality and quantity of intelligence products. It also imposes a kind of order on the whole inventory of methods, techniques and state-of-the-art technologies used to produce intelligence.

A considerable part of intelligence studies has been devoted to the intelligence cycle. As an entry in the *Encyclopedia of Espionage, Intelligence, and Security* (Lerner and Lerner 2004, p. 117) suggests, intelligence is 'intimately tied with the intelligence cycle'. A grand five-volume work on strategic intelligence contains a whole volume— Volume 4—dedicated to the intelligence cycle (Johnson 2007a, b, part 4). Likewise, the *Routledge*

Companion to Intelligence Studies dedicates an entire chapter to this topic (Omand 2013, pp. 59–70). Numerous scholars and practitioners have offered a variety of views, concepts, theoretical models and practical schemes from both historical and contemporary perspectives (Maurer, Turnstall and Keagle 1985; Treverton 2001; Hulnick 2006b; George and Bruce 2008; Evans 2009; Marrin 2009, 2012; Clark 2013; Omand 2013; Phythian 2013a).

The intelligence cycle is a process of transforming raw information and unrefined data into finished intelligence for the use of authorised customers (policy makers). The intelligence cycle is traditionally presented as a process whereby—based on predetermined requirements—raw information is acquired, processed into intelligence and transferred to the authorised users, usually decision makers (Handel 2003, p. 7; Muller 2008).

Stephen Cimbala (1988, p. 73) remarked that: 'What comes out of the intelligence process is a product whose acceptance is not determined by its truth or falsity but by the policymakers' perceived predicaments'. Writ large, the cycle includes tasking, collecting, processing, analysing and disseminating intelligence. It starts with identifying customer needs. Planning and direction are defined based on these requirements in order to manage the entire cycle effectively. The next step is the collection and acquisition of information and data from various sources. Then processing and exploitation takes place; this consists in converting the vast amount of information collected into a form usable by analysts. The next stage refers to the analysis, evaluation and integration of available data with the aim of preparing finished intelligence products. Finally, at the dissemination stage, intelligence products reach the consumers who started the cycle. Quite often, 'soft' intelligence products, devoid of confidential or restricted information, are made available to the public as a way of raising awareness and stimulating resilience to the threats identified (Steele 2002; Xu 2007; George 2008; Lowenthal 2008).

Despite the enormous popularity and application of this concept, there has been no shortage of voices in recent years proclaiming the need for a thorough revision of the classical understanding of the intelligence cycle in a direction that would meet the challenges of the profound technological, civilisational, informational and socio-cultural changes that have occurred since the beginning of the present century. A volume edited by Mark Phythian (2013a), devoted entirely to the search for new concepts, meanings and understandings of the intelligence cycle, contains a rich panorama of theoretical enquiries and practical observations. It also offers a critical assessment of an earlier proposal to re-examine or reconsider the traditional concept of intelligence cycle consisting of five stages: planning and direction, collection, processing, production and analysis, and dissemination (Johnson et al. 2009, p. 34). It was commonly thought that this model was an over-theorised, in some cases simply idealistic, approach to the complex issue of information management. Such a simplified understanding seems fairly limited and fails to adequately capture the dynamics and attributes of the core intelligence process.

One of the early alarms alerting scholars and practitioners that 'something is rotten in the intelligence cycle' was Arthur Hulnick's widely discussed paper (Hulnick 2006a). He argued that the traditional intelligence cycle was a flawed concept and poor theory. He offered an alternative to the traditional view of how intelligence works. In this regard, he referred to counter-intelligence activities and based his cycle on five functions: (1) identification, (2) penetration, (3) exploitation, (4) interdiction, and (5) claiming success (Hulnick 2006a, p. 973).

Loch Johnson observed that the intelligence cycle is more a complex matrix of back-and-forth interactions between intelligence officers and policy officials than a series of smoothly concatenated actions. This matrix, saturated with interpersonal and bureaucratic relationships and patterns, is characterised by 'interruptions, midcourse corrections, and multiple feedback loops'(Johnson et al. 2009, p. 34). For some scholars, the classical intelligence cycle is no longer plausible as part of the intelligence process. Gill and Phythian (2006, pp. 3–4) proposed a distinct approach to information collection and analysis. They described their model as the 'funnel of causality'. They make the point that 'not all information is necessarily translated via analysis into policy, and that much is filtered out' (Gill and Phythian 2006, p. 3).

This conceptualisation has stimulated further enquiry into the substance of the intelligence cycle in the context of the rapidly changing security environment and the emergence of new intelligence disciplines exploring the massive production of information and knowledge. CIA analyst Rob Johnston recommended that: 'The traditional Intelligence Cycle model should either be redesigned to depict accurately the intended goal or care should be taken to discuss explicitly its limitations whenever it is used. […] If the objective is to capture the entire intelligence process, from the request for a product to its delivery, including the roles and responsibilities of Intelligence Community members, then more is required. This should be a model that pays particular attention to representing accurately all the elements of the process and the factors that influence them' (Johnston 2005, p. 55). He built a complex systems model of the intelligence cycle, based on four fundamental intra-systemic actions and relationships: stocks, flows, converters and connectors. These variables determine every stage of the cycle, showing cause-and-effect connections and interdependencies. For Johnston, the logic and cohesiveness of the entire system are decisive for its efficiency and productivity. The role of analysts is highlighted, for they are considered a crucial element of the cycle in terms of actions, capabilities, outcomes and influences (Johnston 2005, pp. 50–4).

Another interesting conceptual proposal was put forward by Geraint Evans. He formulated a revised model, called the hub-and-spoke intelligence cycle, mostly based on military intelligence solutions and experiences. The cycle is composed of eight stages which constantly interact with the operational environment and a command's plans and intentions. Continuous assessment at each one of the stages avoids the blurring or duplication of intelligence efforts (Evans 2009, pp. 41–3).

Strategic Intelligence: A Conceptual Reassessment

The present monograph builds on the thesis that the European Union has facilitated the establishment of an intelligence community operating on the strategic level and exploring mostly open sources of information and intelligence. It is, then, necessary to present the notion of strategic intelligence based on the reassessment of views and concepts existing in the literature on intelligence studies.

There is a general consensus that intelligence activities may be divided into four types:

- Strategic—entailing global and sectoral situational analysis, threat assessment and risk analysis, anticipation of threats and challenges coming from adversaries and competitors.
- Warning—threat and risk warning, crisis management at the early warning stage, foreseeing and alerting discontinuities in preparedness and resilience.
- Operational—support for planning and conduct, crisis response, criminal analysis, intelligence-led actions, loss and damage assessment.
- Tactical—targeting, command and control, surveillance, real-time operation picture, investigation. (Waltz 2003, p. 13; Treverton 2005, p. xi)

Certainly, these types of intelligence are interconnected, often very closely, and in certain circumstances, such as an early warning system or in anti-terror operational planning, mutually enhance the available capacities and means of action. Simon Robertson, former head of the Europol Analysis Unit, noted that 'Although operational and strategic intelligence analysis have different aims, they are mutually dependent and cannot be carried out in isolation. Attempts to separate them, or to foster one at the expense of the other, will result in a fundamentally flawed intelligence programme and a failure to generate meaningful assessments of criminal activity' (Robertson 1997, p. 23).

However, a strategic level of intelligence activities implies a macro approach to the top issues on the security agenda and ensures direct and indirect links to operational and tactical aspects of ongoing processes and developments (Kozłowski and Palacios-Coronel 2014, p. 11). It delivers a 'big picture' (Gutjahr 2005, p. 8). What this macro approach means in theory and practice is a bone of contention among scholars and practitioners. John G. Heidenrich, former analyst of the US Defense Intelligence Agency, even dared to pose a provocative question: '*Does Anyone Know What Strategic Intelligence Is*?' (Heidenrich 2007, p. 25). Seeking an adequate response, one has to see this topical issue in a wider, historical perspective.

Sherman Kent, often described as 'the father of intelligence analysis', the author of the landmark book *Strategic Intelligence for American World Policy*, defined strategic intelligence as 'the knowledge which our highly placed civilians and military men must have to safeguard the national welfare'.[5] This classical standpoint formulated by one of the founders of the US intelligence community should be seen in the context of America's grand strategy, mapped out on the threshold of the Cold War to contain and deter Soviet power. It operated on the strategic level and was preoccupied with long-term objectives and future challenges. With this aim, the intelligence apparatus was hierarchically ordered and bureaucratised, and relied on clandestine sources of information obtained using technical collection devices and processed according to cyclical predictive reasoning. Bruce Berkowitz and Allan Goodman (1989, p. 4) grasped such an understanding of strategic intelligence well, asserting that it aimed 'to provide officials with the "big picture" and long-range forecasts they need in order to plan for the future'.

The evolution of the Cold War security system towards a more complex and interrelated set of actors pursuing their individual strategies and security policies through varied and quite sophisticated ways and means, had a considerable impact on the meaning and practice of intelligence. In the strategic context, it extended its reach on decision-making processes as well as prevention and preparedness for non-military risks and threats. General knowledge of strategic interests and objectives was not enough; it had to be supplemented by operational blueprints, even tactical plans enabling an adequate and effective response to security problems and challenges emerging from the increasingly complex security environment. This became particularly relevant at the turn of the 1980s and 1990s, with a paradigm shift in global and regional security systems. Adda Bozeman (1992, p. 2) encapsulated the essence of strategic intelligence in that special period of international relations. She asserted that the basic function of strategic intelligence is to 'facilitate the steady pursuit of long-range policy objectives even as it also provides guidance in the choice of tactically adroit ad hoc responses to particular occurrences in foreign affairs'.

The meaning of strategic intelligence since the end of the Cold War has undergone considerable evolution, with the centre of analysis shifting towards non-military threats as well as socially, culturally and economically embedded sources of risks and perils. Alessandro Politi, a scholar who conducted research on EU intelligence cooperation in the late 1990s, seems to be perfectly right when claiming that: 'Intelligence has acquired considerably more importance than it had during the Cold War. Whereas before it was needed to maintain the balance of terror, prevent a war in Europe and spot sources of possible politico-military confrontation in the Third World, its tasks now are much wider and more varied, since it helps politicians to steer their national course towards a new world order, new power constellations and economic developments, while avoiding new and old risks' (Politi 1998a, p. 7).

Changing domestic and transnational threats in the post-Cold War era have had a considerable impact on the concept, theory and practice of strategic intelligence, yet they were not powerful enough to turn the traditional approach aside. Basic functions and objectives of strategic intelligence have remained fundamentally unchallenged, demanding from intelligence services deeper information gathering, better data selection and processing and 'sharper' intelligence products. It is the international environment and security structures, however, that have undergone profound changes and produced new challenges and tasks. Global communication networks have expanded hugely, enabling the transmission of unimaginable amounts of data. Social networks began to take advantage of new communication technologies as a way of strengthening interpersonal relations and links. Social media fomented a tremendous proliferation of personal data, including sensitive and valuable information coveted by intelligence services. The Internet was perceived as an information cornucopia allowing for a multi-level strategic assessment that could underpin further preventive and repressive activities against enemies of the state. Open sources came to be treated as the dominant stock of publicly acquired information and data with critical relevance for the intelligence cycle. Advanced technologies and state-of-the-art devices, instruments and programmes reinforced the primary role assigned to signals intelligence by the executive authorities of major global powers (Rolington 2013, pp. 42–52).

Strategic intelligence, then, had to adjust from traditional, enduring objectives to abundant sources of information and data collected, processed and interpreted with the use of advanced digital technologies and computerised tools. After 9/11, the pressure on intelligence services reached a climax and brought about wide theoretical and practical repercussions. In academic terms, the post-9/11 heat gave a boost to intelligence studies and resulted in numerous valuable works on vital theoretical, methodological and educational issues. Strategic intelligence was by no means sidelined by those in the mainstream of the debate. On the contrary, it prompted several important and valuable contributions by outstanding scholars in the field, with a five-volume collection edited by Loch Johnson (2007a) at the forefront.

Loch Johnson and James Wirtz edited an important anthology in which they defined strategic intelligence as that which ‘contributes to the processes, products, and organizations used by senior officials to create and implement national foreign and defense policies. Strategic intelligence thus provides warnings of immediate threats to vital national security interests and assesses long-term trends of interest to senior government officials’ (Johnson and Wirtz 2004, p. 2). Strategic intelligence is underpinned by the core national interests and the sources of state power (Van Cleave 2007, p. 1). This assumption is present in many important contributions to the discussion and the framing of the contested concept of strategic intelligence.

There is a common supposition that intelligence should be focused on the fundamental strategic aspects of national security, public order and international developments. This aspect was emphasised by Heidenrich (2007, p. 15), who maintained that ‘Strategic intelligence is essential […]

for it constitutes nothing less than the integral intelligence support of a strategy, very often the national strategy'. Richard Russell emphasised 'grand strategy', comprising the realms of power, force and politics. He conceived of intelligence as a strategic asset guaranteeing fundamental national interests. He wrote: 'Strategic intelligence is the use of information, whether clandestinely or publicly acquired, that is synthesised into analysis and read by the senior-most policy makers charged with setting the objectives of grand strategy and ensuring that military force is exercised for purposes of achieving national interests' (Russell 2007a, p. 6). In a similar vein Stephen Marrin (2011, p. 9) argued that 'The strategic analyst requires an ability to critically evaluate a situation, assess it for significance, match the assessment of significance against either decisionmaker interest or national interest, reframe or re-conceptualize the situation as needed, and construct an argument about that significance using whatever information, including raw intelligence, is available'.

Another approach highlights the dynamics of strategic intelligence, an active interplay of elements of information gathering and analytical skills in the framework of policy making and effective governance. Thomas Fingar (2011, p. 53) argued that the main objective of strategic intelligence is 'to identify the most important streams of developments, how they interact, where they seem to be headed, what drives the process, and what signs might indicate a change of trajectory. Stated another way, strategic analysis seeks to identify the factors that will shape the future so that policy makers can devise strategies and formulate policies to maintain positive trajectories and shift negative ones in a more positive direction. The ultimate goal is to shape the future, not to predict what it will be.'

Another strand of strategic intelligence theory shifts the centre of gravity from the thorough assessment of the national security environment based on comprehensive knowledge towards situational awareness and anticipation of emerging threats and risks entailing an extensive foreknowledge, to use Kirkpatrick's (1997, p. 365) well-known phrasing. The value of strategic intelligence lies in its predictive capacity, anticipatory power and early warning capability, which facilitate policy planning, strategic assessment and proper understanding of ongoing developments and future trends (Sullivan 2007, p. 17). Julian Richards (2010, p. 23) points out this feature of strategic intelligence, noting that it 'aims to be more forward-looking and predictive'. He adds that this sort of intelligence is hard and demanding because it consists of the 'use of analysis of fragmented information and modelling of past activities and behaviours to predict what might happen in the future' (Richards 2010, p. 23). John P. Sullivan (2007, p. 17) also recognises the relevance of threat anticipation and forecast in a global networked environment. He writes: 'Intelligence is more about early warning, strategic foresight, and real-time decision support for cooperative risk management than about gaining a secret advantage over a single state adversary.' Strategic intelligence focuses on long-term aims, entailing the use of ordinary and advanced methods and tools of projection, foreknowledge and precognition (Strang 2014, p. 2). Strategic intelligence leads to a general review of available knowledge about current and emerging trends, changes in the security environment, threats and risks. It also advocates preventing and countering negative consequences of insecurity through legal and political programmes and decisions (Sullivan 2007, pp. 22–3; Europol 2000, p. 29). In other words, strategic intelligence often seeks to reduce long-term vulnerabilities to emerging threats and hazards through 'strategic collection against future threats and the analysis of macrotrends' (Sims 2005, p. 15).

Strategic intelligence is an integral part of national security policies and international cooperation. It supports states and their societies in tackling crucial challenges to their security, order and well-being. It entails advanced, often sophisticated, intelligence methods and analytical tools. As Wheaton (2011, p. 367) noticed, it is 'the highest form of the analytic art'. It has to cope effectively with the growing need on the part of the major customers, especially governments and state authorities responsible for security policies, as well as international organisations, for a comprehensive, accurate, updated 'macro-depiction' of the security environment containing specific highlights and warnings about the future as well as imminent threats, perils and pitfalls. Under current conditions, in the global, networked, interconnected world, strategic intelligence responds to the increasingly complex and challenging task of effective security governance.

The Transnational Intelligence Community

The intelligence community may be simply defined as a set of interlocking units, agencies and organisations that carry out intelligence activities for a decision-making body. When elevated to transnational level, the intelligence community is subject to two basic prerequisites of international intelligence cooperation. One is positive and reflects favourable attitudes existing among actors who share values, ideas, interests and objectives. In a symbiotic environment cooperation among intelligence agencies, services and officers is considered logical and natural. It proves to be sincere, efficient, reliable, accountable and beneficial on the grounds of common strategic interests, congenial ideological bases, like-minded attitudes to national interests and global determinants. It therefore needs robust bilateral or multilateral interconnections built and developed harmoniously with a strong sense of belonging to the same security community.

The other prerequisite has a negative flavour because it addresses concerns, uncertainties, threats and challenges posed by a hostile environment, defiant 'rogue' actors, fragile security structures and proliferating risks and perils. The unpredictability and contingency of threats and hazards brings the affected actors together and fosters mutual cooperative patterns. The fear of a breakdown, disruption or crisis which might provoke damaging and far-reaching consequences for security and order is a factor stimulating information exchange, knowledge sharing and intelligence collaboration. Although this cooperation may be relatively weak and sometimes provisional and short-lived, it is usually consolidated against the common threats and security dilemmas. Hence, it is relatively durable and long-standing as long as the vital threats and crucial security challenge persist. However, if they appear frequently and regularly, forcing the affected actors to react and take joint action, they can contribute to the emergence and consequent consolidation of collaborative frameworks, patterns and arrangements enhancing the power of response to problematic security issues (Lander 2004, pp. 490–3; Clough 2004, pp. 605–7; Wippl 2012, pp. 7–12; Munton and Fredj 2013, pp. 668–70).

The experience of EU integration has shown that these two approaches can intermingle and bring about a relatively strong, efficient and robust intelligence cooperation structure. The hybrid nature of the European Union facilitates the co-existence of weak, ad hoc and makeshift arrangements with stable, institutionalised, cohesive set-ups. Still, the national sovereignty principle is the security benchmark testing the plausibility of transnational cooperative structures and mechanisms. The threshold of joint response to a disruption or a crisis is set at the intersection of national security objectives and measures adopted by every single Member State and common institutional capability to react to a crisis at the EU level. The coherence and effectiveness of the EU intelligence community is therefore greatly determined by Member States' confidence in the capability and strength of the European Union when coping with vital threats and huge challenges to national security, public order or the well-being of its members.

A theoretical as well as practical view of the framework, substance and internal architecture of the intelligence community has been strongly predetermined by the US model. A considerable part of the scholarship in intelligence studies has been devoted to the US intelligence community (Flanagan 1985; Boren 1992; Hulnick 1999; Zegart 1999; Kindsvater 2003; Staar 2003; Betts 2007; Lowenthal 2008; Richelson 2012). This community is in any case a national intelligence organisation, despite having a mildly hierarchical, federation-like structure which resembles international intelligence arrangements. In this case, one gets the feeling that its internal links and ties are rather loose and stretched between the numerous agencies and bodies making up the whole community. Alessandro Politi (1998a, p. 8) noticed that an intelligence community 'cannot be the total sum of existing bilateral or multilateral links among agencies'. In a similar vein Antonio Díaz Fernández (2010, p. 230) ascertained that an intelligence community cannot be reduced to 'a mere aggregate of intelligence organizations and the political bodies that consume intelligence'. These remarks are particularly relevant for the study of the EU intelligence community in the context of the adopted network approach and nodal governance. Given that the scholarship on transnational intelligence cooperation is still underdeveloped, it seems legitimate to put forward a conceptualisation responding to the dynamics of the making of international intelligence arrangements.

The cognitive framework adopted in this work has to be widened when transnational network structures are the subject of the research. It leads us to the implementation of concepts that correspond to intelligence community yet have a different content and a wider scope of cognitive utility. The basic supplementary methodological instrument used in our analysis of transnational intelligence community is the concept of epistemic communities. This emerged as an analytical tool on the verge of the post-Cold War transformation of the global order.[6] In 1992 Peter Haas, in his seminal introductory paper in a special issue of *International Organization*, a leading journal covering the entire field of international relations, defined epistemic communities as a 'network of professionals with recognized expertise and competence in a particular domain and an authoritative claim to policy-relevant knowledge within that domain or issue-area' (Haas 1992a, p. 3). These professionals share causal and principled beliefs, policy-relevant expertise, criteria for validating knowledge in their area of expertise and practices associated with problems in which their competence is addressed (Haas 1989, pp. 384–5).

In practical terms, epistemic communities can be conceived of as policy-driven advisory groups, often of transnational provenance, influential or supportive of decision makers. Haas (1992b, p. 188) argued that 'the epistemic community was largely responsible for identifying and calling attention to the existence of a threat […] and for selecting policy choices'. In another paper, he claimed that 'Epistemic communities may introduce new policy alternatives to their governments, and depending on the extent to which these communities are successful in obtaining and retaining bureaucratic power domestically, they can often lead their governments to pursue them' (Haas 1989, p. 402).

An epistemic community is a network of agents with privileged access to information and/or knowledge crucial for the optimisation of the decision-making process and its outcomes (Galbreath and McEvoy 2013, pp. 173–4). The community rests on a cohort of top experts and specialists in a given area. The sources of information and knowledge may take the form of data bases, libraries, archives, big-data storage platforms etc. Some of these sources are restricted and access to them requires authorisation. In this respect, the epistemic community is formed by highly skilled professionals endowed with special capabilities and experience in managing information and knowledge. Its role consists in providing decision makers with processed information or a kind of expertise which is then reprocessed, evaluated and used by them as optimisation solutions. Haas argued that epistemic communities cannot rely on guesses or 'raw' information; they have to seek different information and data acquired from various sources in order to draw a broad picture made of judgments, interpretations and reflections on social and physical phenomena.

Epistemic communities in the original Hassian and Adlerian conceptualisation were conceived of as vertically oriented heterogeneous institutionalised networks formed to influence decision-making processes and policy outcomes (Sebenius 1992, p. 325). This conceptualisation contained an important caveat: epistemic communities emerge, exist and act outside the scope of decision-making institutions and processes. They can stimulate debate, formulate alternatives, share views and opinions and offer policy learning. Yet they do not participate in the actual act of making critical choices that have far-reaching implications and imply political responsibility. In this respect, epistemic communities consist of 'outsiders', belonging in the decision environment yet not part of the decision unit (Mintz and DeRouen Jr. 2010, p. 18). Haas (1992a, p. 15) excluded policy makers and leaders from membership in epistemic communities because their partisanship and advocacy is in sharp contrast to the professional roles of civil servants, who are considered 'technicians, policymakers and brokers'.

An intelligence community is a kind of epistemic community but its structure, organisation and internal logic are highly specific and adjusted to political and security needs. So, one can call a transnational intelligence community a distorted epistemic community because of its tendency to process and analyse information on the basis of an all-source approach (due to the limited access to secret assets) in a flattened networked configuration (because of the lack of a central authority) relying on technological solutions to data acquisition, processing and transmission (due to the lack or deficit of human intelligence). The distorted epistemic community builds on transverse connections between various stakeholders, including governments, private entities and supranational actors. It seeks to integrate scattered sources of information and knowledge on the basis of shared interests, values and objectives which contribute to the establishment of a common identity.

The distorted epistemic community model seeks to alleviate the difficulties and compensate for the weaknesses of transnational intelligence cooperation in a complex security environment. It focuses on constructive aspects of intelligence collaboration, highlighting incentives and added values and diminishing negative consequences and side effects, especially for individual participants. Given that intelligence cooperation is substantially politicised, and often subject to strategic guidelines and vital security interests, the distorted epistemic community is engaged in the policy-making process in a direct way, often on a daily basis and when alerted. On the other hand, the information deficits, organisational faults and decision-making bottlenecks inherent in supranational arrangements present a constant challenge for the members of the intelligence community and sometimes bring about serious distortions of the structural and institutional groundwork. The hybrid structure of the distorted epistemic community, encompassing heterogeneous and homogeneous components interacting in organisational hubs, hinders an efficient and flexible response to emerging complications, problems and challenges.

Building an EU Strategic Intelligence Community

The strategic intelligence and international cooperation of the distorted epistemic community, discussed above, clearly show the singular nature of the EU intelligence community project. The basic questions are: how distorted is the EU intelligence community with regard to the classic epistemic communities model, and what are the main causes of distortion and dispersion as regards knowledge management and data processing at EU level? It is worth referring back to the concept of strategic intelligence in our attempt to answer these questions.

Babak Akhgar, Simeon Yates and Eleanor Lockley (2013, p. 6) observed that strategic intelligence needs to meet certain requirements, such as:

- assessment, aimed at addressing global environmental scanning, which includes national strengths, weaknesses, opportunities and threats;
- knowledge and learning processes, which ensure that intelligence is focused on relevant threats and risks and can effectively frame strategic policies, priorities and resourcing, thus giving key support to decision makers;
- a holistic approach to the full range of risks and threats, both internal and external;
- goal- and result-oriented action, stimulating a collaborative approach to tackle specific threats and hazards through the setting of measurable targets;
- an adaptive approach, enabling a quick and flexible response to all new and emerging threats.

A bird's-eye view of a transnational intelligence community, such as that established by the European Union, confirms the existence of the majority of the above elements, although at a different scale and with varied effects. A strategic intelligence community builds on comprehensiveness, regardless of limits and obstacles. All-source analysis is the key method enabling the production of strategic assessments and the building of situational awareness of security issues. The limited access to secret information and protected sources of intelligence is compensated for by networking and intelligence sharing, as well as sophisticated tools and methods applied to open-source analysis. We can then subscribe to Richards' view that 'Secrecy, therefore, is not an inherent aspect of intelligence, but the exclusivity of information can be critical and can make the difference between openly available data and "intelligence" which helps policy-makers take significant action' (Richards 2010, p. 20). While the restricted accessibility to secret intelligence is a serious drawback of the transnational intelligence community, international cooperation and the value added to security policies by transnational linkages and connectivities have a positive effect. It is worth remembering that intelligence services develop and perform certain liaison functions in the international arena (Lefebvre 2003, pp. 536–7; Omand 2010, pp. 103–6). Although they are established on a bilateral basis over time and are subject to the scale of the cooperation between the participating states, stable structural arrangements may emerge at the transnational level, tending to institutionalisation and reciprocity. Since they focus on the 'big picture' of the security environment, they adopt the evidently strategic outlook, keeping particular issues embedded in the national dimension of intelligence security.

Michael Herman (1996, p. 218) noted that 'Intelligence collaboration is the servant of national political objectives, but at a strategic rather than tactical level'. Indeed, the strategic dimension of intelligence cooperation enables the emergence of stable, accountable and effective forms and mechanisms for the gathering, collation, analysis and exchange of information and analytical materials. Expectations of reliable information and accurate intelligence have risen to the extent that national intelligence services have strengthened formal and informal ties and begun to make use of certain multilateral fora facilitating closer cooperation. The European Union is the most telling example of a far-ranging forum contributing to the realisation of the vital security interests of its Member States without neglecting the strategic guidelines and supranational policies of the EU as a whole.

Notes

1. For a critical view of the rational bases of strategy, see Betts (2000, pp. 5–50).
2. These parameters were identified and introduced into the study of international relations by Roberta Wohlstetter in a memorandum for the Office of the Assistant Secretary of State and published by the Rand Corporation. See Wohlstetter (1965a). Excerpts from this memorandum were later published as an article for the journal *Foreign Affairs*. See Wohlstetter (1965b).
3. However, Alan Breakspear proposed a new definition of intelligence in which the nexus between intelligence and secrecy was dismissed as a defining element of intelligence. See Breakspear (2013, p. 685).
4. Lord Dacre as quoted by Trevor-Roper (1968, p. 66), quoted in Herman (1996, p. 88).
5. Kent (1966), p. vii.
6. Actually the origins of the concept of epistemic communities can be traced back to the late 1960s and early 1970s when the debate on the epistemological and cognitive properties of IR theory began. See Haas (1992a, pp. 3–4), Antoniades (2003, p. 23), Davis Cross (2013a, pp. 141–2; 2013b, pp. 46–8; 2015, pp. 91–3).

Bibliography

Agrell, W. (2002). *When everything is intelligence—Nothing is intelligence*. The Sherman Kent center for intelligence analysis occasional papers, 1(4). At https://www.cia.gov/library/kent-center-occasional-papers/vol1no4.htm. Accessed 14 Sept 2012.

Agrell, W., & Treverton, G. F. (2015). *National intelligence and science. Beyond the great divide in analysis and policy*. Oxford/New York: Oxford University Press.

Akhgar, B., Yates, S., & Lockley, E. (2013). Introduction: Strategy formation in a globalized and networked age—A review of the concept and its definition. In B. Akhgar & S. Yates (Eds.), *Strategic intelligence management. National security imperatives and information and communications technologies*. Waltham/Kidlington: Butterworth-Heinemann.

Altshuler, Y., et al. (Eds.). (2013). *Security and privacy in social networks*. New York/Heidelberg/Dordrecht/London: Springer.

Antoniades, A. (2003). Epistemic communities, epistemes and the construction of (world) politics. *Global Society, 17*(1), 21–38.

Babcock, C. (2010). *The cloud revolution. How cloud computing is transforming business and why you can't afford to be left behind*. New York/Chicago/San Francisco: McGraw-Hill.

Bamford, P. (2004). *Pretext for war: 9/11, Iraq, and the abuse of America's intelligence agencies*. New York: Doubleday.

Barger, D. G. (2005). *Toward a revolution in intelligence affairs*. RAND Technical Report TR-242. Santa Monica: RAND Corporation.

Bean, H. (2011). *No more secrets: Open source information and the reshaping of U.S. intelligence*. Santa Barbara/Denver/London: Praeger.

Ben-Zvi, A. (1976). Hindsight and foresight: A conceptual framework for the analysis of surprise attack. *World Politics, 28*(3), 381–395.

Berkowitz, B. D., & Goodman, A. E. (1989). *Strategic intelligence for American national security*. Princeton: Princeton University Press.

Betts, R. K. (2000). Is strategy an illusion? *International Security, 25*(2), 5–50.

Betts, R. K. (2003). Politicization of intelligence: Costs and benefits. In R. K. Betts, & Th. G. Mahnken (Eds.), *Paradoxes of strategic intelligence: Essays in honor of Michael I. Handel*. London: Frank Cass.

Betts, R. K. (2007). *Enemies of intelligence: Knowledge and power in American national security*. New York/Chichester: Columbia University Press.

Blanken, L. J. (2012). Reconciling strategic studies … with itself: A common framework for choosing among strategies. *Defense & Security Analysis, 28*(4), 275–287.

Boren, D. L. (1992). The intelligence community: How crucial? *Foreign Affairs, 71*(3), 52–62.

Bozeman, A. B. (1992). *Strategic intelligence & statecraft: Selected essays.* Washington, DC: Brassey's.

Bowman, E. C. (2012). *Intelligence, Surveillance, and Reconnaissance Processing, Exploitation, and Dissemination System in Support of Global Strike in 2035.* Maxwell AFB: Air War College.

Breakspear, A. (2013). A new definition of intelligence. *Intelligence and National Security, 28*(5), 678–693.

Brown, S. D. (2007). The meaning of criminal intelligence. *International Journal of Police Science & Management, 9*(4), 336–340.

Button, M. (2008). *Doing security. Critical reflections and an agenda for change.* Basingstoke/New York: Palgrave Macmillan.

Cimbala, S. J. (1988). Amorphous wars. *International Journal of Intelligence and Counterintelligence, 2*(1), 73–89.

Clark, R. M. (2013). *Intelligence analysis: A target-centric approach* (4th ed.). Thousand Oaks: CQ Press.

Clough, C. (2004). Quid Pro Quo: The challenges of international strategic intelligence cooperation. *International Journal of Intelligence and CounterIntelligence, 17*(4), 601–613.

Collins, J. M. (2002). *Military strategy: Principles, practices, and historical perspectives.* Washington, DC: Potomac Books.

Dahl, E. J. (2011). The plots that failed: Intelligence lessons learned from unsuccessful terrorist attacks against the United States. *Studies in Conflict and Terrorism, 34*(8), 621–648.

Davis, J. (2002). *Sherman Kent and the profession of intelligence analysis.* The Sherman Kent Center for Intelligence Analysis Occasional Papers, 1(5). At https://www.cia.gov/library/kent-center-occasional-papers/vol1no5.htm. Accessed 18 Dec 2011.

Davis Cross, M. K. (2013a). Rethinking epistemic communities twenty years later. *Review of International Studies, 39*(1), 137–160.

Díaz Fernández, A. M. (2010). The Spanish intelligence community: A diffuse reality. *Intelligence and National Security, 25*(2), 223–244.

Dupont, A. (2003). Intelligence for the twenty-first century. *Intelligence and National Security, 18*(4), 15–39.

Einstein, A. (1954). *Ideas and opinions.* New York: Crown Publisher.

Europol. (2000). *Analytical guidelines.* The Hague: Europol.

Evans, G. (2009). Rethinking military intelligence failure—Putting the wheels back on the intelligence cycle. *Defence Studies, 9*(1), 22–46.

Fingar, T. (2011). *Reducing uncertainty: Intelligence analysis and national security.* Stanford: Stanford University Press.

Flanagan, S. J. (1985). Managing the intelligence community. *International Security, 10*(1), 58–95.

Freedman, L. (2013). *Strategy. A history.* Oxford: Oxford University Press.

Galbreath, D. J., & McEvoy, J. (2013). How epistemic communities drive international regimes: The case of minority rights in Europe. *Journal of European Integration, 35*(2), 169–186.

George, R. Z. (2008). The art of strategy and intelligence. In R. Z. George & J. B. Bruce (Eds.), *Analyzing intelligence: Origins, obstacles, and innovations.* Washington, DC: Georgetown University Press.

George, R. Z., & Bruce, J. B. (Eds.). (2008). *Analyzing intelligence: Origins, obstacles, and innovations.* Washington, DC: Georgetown University Press.

Gibson, S.D. (2004). Open Source Intelligence: An Intelligence Lifeline. *Royal United Services Institute Journal, 149*(1), 16–22.

Gill, P. (2004). Securing the globe: Intelligence and the post-9/11 shift from 'liddism' to 'drainism'. *Intelligence and National Security, 19*(3), 467–489.

Gill, P., & Phythian, M. (2006). *Intelligence in an insecure world.* Cambridge: Polity Press.

Gill, P., & Phythian, M. (2012). *Intelligence in an insecure world* (2nd ed.). Cambridge: Polity Press.

Gupta, R., & Brooks, H. (2013). *Using social media for global security.* Indianapolis: Wiley.

Gutjahr, M.M.H. (2005). *The Intelligence Archipelago: The Community's Struggle to Reform in the Globalized Era*. Washington, DC: Joint Military Intelligence College.

Haas, P. M. (1989). Do regimes matter? Epistemic communities and Mediterranean pollution control. *International Organization, 43*(3), 377–403.

Haas, P. M. (1992a). Introduction: Epistemic communities and international policy coordination. *International Organization, 46*(1), 1–35.

Haas, P. M. (1992b). Banning chlorofluorocarbons: Epistemic community efforts to protect stratospheric ozone. *International Organization, 46*(1), 187–224.

Hall, W. M., & Citrenbaum, G. (2010). *Intelligence analysis: How to think in complex environments.* Santa Barbara: ABC-CLIO.

Handel, M. (1987). The politics of intelligence. *Intelligence and National Security, 2*(4), 5–46.

Handel, M. I. (2003). Intelligence and the problem of strategic surprise. In R. K. Betts & Th. G. Mahnken (Eds.), *Paradoxes of strategic intelligence: Essays in honor of Michael I. Handel.* London: Frank Cass.

Heidenrich, J. G. (2007). The Intelligence Community's Neglect of Strategic Intelligence. *Studies in Intelligence, 51*(2), 15-26.

Herman, M. (1996). *Intelligence power in peace and war.* Cambridge: Cambridge University Press.

Herrera, L. (2014). *Revolution in the age of social media: The Egyptian popular insurrection and the internet.* London/New York: Verso.

Heuser, B. (2010). *The evolution of strategy: Thinking war from antiquity to the present.* Cambridge: Cambridge University Press.

Hilsman, R., Jr. (1952). Intelligence and policy-making in international affairs. *World Politics, 5*(1), 1–45.

Hilsman, R. (1956). *Strategic intelligence and national decisions*. Glencoe: The Free Press.

Hulnick, A. S. (1999). *Fixing the spy machine: Preparing American intelligence for the 21st century*. Westport: Praeger.

Hulnick, A. S. (2006a). What's wrong with the intelligence cycle. *Intelligence and National Security, 21*(6), 959–979.

Hulnick, A. S. (2006b). U.S. intelligence reform: Problems and prospects. *International Journal of Intelligence and CounterIntelligence, 19*(2), 302–315.

Jablonsky, D. (2004). Why is strategy difficult? In J. B. Bartholomees Jr. (Ed.), *U.S. Army War College guide to national security policy and strategy*. Strategic Studies Institute, U.S. Army War College: Carlisle.

Jeffreys-Jones, R. (2011). Rise, fall and regeneration: From CIA to EU. In L. Scott, R. G. Hughes, & M. S. Alexander (Eds.), *Intelligence and international security. New perspectives and agendas*. London/New York: Routledge.

Jervis, R. (2006). Reports, politics, and intelligence failures: The case of Iraq. *Journal of Strategic Studies, 29*(1), 3–52.

Johnson, L. K. (Ed). (2007a). *Strategic intelligence*, 4 vols. Westport/London: Praeger Security International.

Johnson, L. K. (Ed). (2007b). *Handbook of intelligence studies*. London/New York: Routledge.

Johnson, L. K., & Wirtz, J. J. (Eds.). (2004). *Strategic intelligence: Windows into a secret world*. Los Angeles: Roxbury.

Johnson, J. L., Kartchner, K. M., & Larsen, J. A. (2009). Introduction. In J. L. Johnson, K. M. Kartchner, & J. A. Larsen (Eds.), *Strategic culture and weapons of mass destruction: Culturally based insights into comparative national security policymaking*. London/New York: Palgrave Macmillan.

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

Kahn, D. (2009). An historical theory of intelligence. In P. Gill, S. Marrin, & M. Phythian (Eds.), *Intelligence theory. Key questions and debates*. Abingdon/New York: Routledge.

Kendall, W. (1949). The function of intelligence. *World Politics, 1*(4), 542–552.

Kent, S. (1966). *Strategic intelligence for American world policy*. Princeton: Princeton University Press.

Kindsvater, L. C. (2003). The need to reorganize the intelligence community: A senior officer's perspective. *Studies in Intelligence, 47*(1), 33–37.

Kirkpatrick, Jr., L. B. (1997). Intelligence. In B. W. Jentleson & Th. G. Paterson (Eds.), *Encyclopedia of US foreign relations*, vol. 2. Oxford/New York: Oxford University Press.

Kozłowski, J., & Palacios-Coronel, J.-M. (2014). Single Intelligence Analysis Capacity (SIAC)—A part of the EU comprehensive approach. *Impetus. Magazine of the EU Military Staff, 17*, 10–11.

Lander, S. (2004). International intelligence cooperation: An inside perspective. *Cambridge Review of International Affairs, 17*(3), 481–493.

Laqueur, W. (1985). *A world of secrets: The uses and limits of intelligence.* New York: Basic Books.

Lefebvre, S. (2003). The difficulties and dilemmas of international intelligence cooperation. *International Journal of Intelligence and CounterIntelligence, 16*(4), 527–542.

Lerner, K. L., & Lerner, B. W. (2004). Tradecraft. In K. L. Lerner & B. W. Lerner (Eds.), *Encyclopedia of espionage, intelligence, and security* (Vol. 3). Detroit: Thomson Gale.

Lowenthal, M. M. (2008). *Intelligence: From secrets to policy* (4th ed.). Washington, DC: CQ Press.

Lykke, A. F., Jr. (1989). *Military strategy: Theory and application.* Carlisle: U.S. Army War College.

Manosevitz, J. U. (2013). Needed: More thinking about conceptual frameworks for analysis—The case of influence. *Studies in Intelligence, 57*(4), 15–22.

Marrin, S. (2009). Intelligence analysis and decision-making: Methodological challenges. In P. Gill, S. Marrin, & M. Phythian (Eds.), *Intelligence theory. Key questions and debates.* Abingdon/New York: Routledge.

Marrin, S. (2011). *Improving intelligence analysis. Bridging the gap between scholarship and practics.* London/New York: Routledge.

Marrin, S. (2012). Evaluating the quality of intelligence analysis: By what (mis) measure? *Intelligence and National Security, 27*(6), 896–912.

Maurer, A. C., Turnstall, M. D., & Keagle, J. M. (Eds.). (1985). *Intelligence: Policy and process.* Boulder: Westview Press.

Mercado, S. C. (2004). Sailing the sea of OSINT in the information age. *Studies in Intelligence, 48*(3), 45–55.

Mintz, A., & DeRouen, K., Jr. (2010). *Understanding foreign policy decision making.* Cambridge: Cambridge University Press.

Moore, D. T. (2007). *Critical thinking and intelligence analysis.* Occasional Paper No. 14. Washington, DC: National Defense Intelligence College.

Muller, D. G., Jr. (2008). Intelligence analysis in red and blue. *International Journal of Intelligence and CounterIntelligence, 21*(1), 1–12.

Munton, D., & Fredj, K. (2013). Sharing secrets: A game theoretic analysis of international intelligence cooperation. *International Journal of Intelligence and CounterIntelligence, 26*(4), 666–692.

Nicander, L. D. (2011). Understanding intelligence community innovation in the post-9/11 world. *International Journal of Intelligence and CounterIntelligence, 24*(3), 534–568.

Olcott, A. (2014). *Open source intelligence in a networked world.* London/New York: Continuum.

Omand, D. (2010). Creating intelligence communities. *Public Policy and Administration, 25*(1), 99–116.

Omand, D. (2013). The intelligence cycle. In R. Dover, M. S. Goodman, & C. Hillebrand (Eds.), *Routledge companion to intelligence studies.* London: Routledge.

Papacharissi, Z. (2009). The virtual geographies of social networks: A comparative analysis of Facebook, LinkedIn and A SmallWorld. *New Media & Society, 11*(1–2), 199–220.

Phythian, M. (2005). Intelligence, policy-making and the 7 July 2005 London bombings. *Crime, Law & Social Change, 44*(4-5), 361–385.

Phythian, M. (Ed.). (2013a). *Understanding the intelligence cycle.* London/New York: Routledge.

Politi, A. (Ed.). (1998a) *Towards a European intelligence policy.* Chaillot Paper No. 34. Paris: Institute for Security Studies of the WEU.

Rathmell, A. (2002). Towards postmodern intelligence. *Intelligence and National Security, 17*(3), 87–104.

Richards, J. (2010). *The art and science of intelligence analysis.* Oxford/New York: Oxford University Press.

Richelson, J. T. (1999). *The U.S. intelligence community* (4th ed.). Boulder/Oxford: Westview Press.

Richelson, J. T. (2012). *The U.S. intelligence community* (6th ed.). Boulder: Westview Press.

Robertson, S. (1997). Intelligence-led policing: A European Union view. In A. Smith (Ed.), *Intelligence-led policing. International perspectives on policing in the 21st century.* Lawrenceville: IALEIA.

Rolington, A. (2013). *Strategic intelligence for the 21st century. The mosaic method.* Oxford: Oxford University Press.

Rovner, J. (2011). *Fixing the facts: National security and the politics of intelligence.* Ithaca: Cornell University Press.

Rovner, J. (2013). Is politicization ever a good thing? *Intelligence and National Security, 28*(1), 55–67.

Russell, R. L. (2007a). *Sharpening strategic intelligence. Why the CIA gets it wrong, and what needs to be done to get it right.* Cambridge/New York: Cambridge University Press.

Sebenius, J. K. (1992). Challenging conventional explanations of international cooperation: Negotiation analysis and the case of epistemic communities. *International Organization, 46*(1), 323–365.

Shelton, C. (2011). The roots of analytic failures in the U.S. Intelligence community. *International Journal of Intelligence and CounterIntelligence, 24*(4), 637–655.

Sims, J. E. (2005). Understanding friends and enemies: The context for American intelligence reform. In J. E. Sims & B. Gerber (Eds.), *Transforming US intelligence.* Washington, DC: Georgetown University Press.

Staar, R. F. (2003). The US intelligence community. *Review of Policy Research, 20*(4), 713–726.

Steele, R. D. (2002). *The new craft of intelligence. Personal, public, & political.* Oakton: OSS International Press.

Strang, S. J. (2014). Network analysis in criminal intelligence. In A. J. Masys (Ed.), *Networks and network analysis for defence and security*. Heidelberg: Springer.

Sullivan, J. P. (2007). The new great game: Military, police and strategic intelligence for global security. *Journal of Policing, Intelligence and Counter Terrorism, 2*(2), 15–29.

Terranova, T. (2004). *Network culture: Politics for the information age*. Ann Arbor: Pluto Press.

Treverton, G. F. (2001). *Reshaping national intelligence in an age of information*. Cambridge: Cambridge University Press.

Treverton, G. F. (2005). Foreword. In R. Johnston (Ed.), *Analytic culture in the US intelligence community*. Washington, DC: The Center for the Study of Intelligence.

Treverton, G. F. (2009). *Intelligence for an age of terror*. Cambridge/New York: Cambridge University Press.

Trottier, D. (2012). *Social media as surveillance: Rethinking visibility in a converging world*. Farnham/Burlington: Ashgate.

Tucker, D. (2014). *The end of intelligence: Espionage and state power in the information age*. Stanford: Stanford University Press.

Turner, S. (1991). Intelligence for a new world order. *Foreign Affairs, 70*(4), 150–166.

Van Cleave, M. (2007). Strategic counterintelligence: What is it, and what should we do about it? *Studies in Intelligence, 51*(2), 1–13.

Walters, V. (1978). *Silent missions*. Garden City: Doubleday.

Waltz, E. (2003). *Knowledge management in the intelligence enterprise*. Boston/London: Artech House.

Warner, M. (2009). Intelligence as risk shifting. In P. Gill, S. Marrin, & M. Phythian (Eds.), *Intelligence theory. Key questions and debates*. Abingdon/New York: Routledge.

Westerfield, H. B. (1996). America and the world of intelligence liaison. *Intelligence and National Security, 11*(3), 523–560.

Wheaton, K. J. (2011). Teaching strategic intelligence through games. *International Journal of Intelligence and CounterIntelligence, 24*(2), 367–382.

Wheaton, K. J., & Beerbower, M. T. (2006). Towards a new definition of intelligence. *Stanford Law & Policy Review, 17*(2), 319–331.

White, C. M. (2012). *Social media, crisis communication, and emergency management. Leveraging Web 2.0 technologies*. Boca Raton/London/New York: CRC Press.

Wippl, J. W. (2012). Intelligence exchange through interintel. *International Journal of Intelligence and CounterIntelligence, 25*(1), 1–18.

Wohlstetter, R. (1965a). *Cuba and Pearl Harbor: Hindsight and foresight*. Memorandum RM-4328-ISA. Santa Monica: RAND Corporation. At http://www.rand.org/content/dam/rand/pubs/research_memoranda/2007/RM4328.pdf. Accessed 2 Dec 2012.

Wohlstetter, R. (1965b). Cuba and Pearl Harbor: Hindsight and foresight. *Foreign Affairs, 43* (4), 691–707.

Woodard, N. (2013). Tasting the forbidden fruit: Unlocking the potential of positive politicization. *Intelligence and National Security, 28*(1), 91–108.

Xu, M. (Ed.). (2007). *Managing strategic intelligence: Techniques and technologies.* Hershey/London: Information Science Reference.

Xu, M., & Kaye, R. (2007). The nature of strategic intelligence, current practice and solutions. In M. Xu (Ed.), *Managing strategic intelligence: Techniques and technologies*. Hershey/London: Information Science Reference.

Yarger, H. R. (2006). *Strategic theory for the 21st century: The little book on big strategy*. Carlisle: Strategic Studies Institute, U.S. Army War College.

Zegart, A. B. (1999). *Flawed by design: The evolution of the CIA, JCS, and NSC.* Stanford: Stanford University Press.

CHAPTER 3

Intelligence Tradecraft in the European Union

The previous chapter proposed the concept of the EU intelligence community as a sort of distorted epistemic community operating at the transnational strategic level, arguing moreover that the EU strategic intelligence community is made up of networks and institutions operating within a common legal and procedural framework. The hybrid nature of the EU's security makes this framework far from integral, although it moves the focus of analysis away from single components embedded in the given legal-institutional settings. An integrated framework is also helpful in developing other concepts and analytical tools enabling a comprehensive approach to the field under observation.

In the study of intelligence communities, 'tradecraft' is associated with the ability to integrate individual skills, organisational schemes, diversified means and practical solutions—worked out, developed and practised by every single community member—into a common platform of information management and intelligence production. If we take the European Union as a sort of intelligence community, it is tempting to examine cooperation between different stakeholders of the EU intelligence community in terms of 'tradecraft'. Hence, adhering to the strategic perspective adopted here, we will focus on 'intelligence process' and 'intelligence products'; that is, how the ways and means adopted by the stakeholders of the EU intelligence community contribute to the outcomes and 'products' offered to EU Member States and what sort of feedback should be

A. Gruszczak, *Intelligence Security in the European Union*,
DOI 10.1057/978-1-137-45512-3_3

expected from EU agencies and bodies involved in intelligence sharing. It should be underlined that the strategic character of the EU intelligence community is one of analytical tradecraft not related directly to operations involving intelligence officers in field activities. Put simply, the European Union has nothing to do with 'spycraft'—the inventory of special techniques, methods, tools and devices applied to the gathering of predominantly secret information held by other states or foreign services (Davies 2005). Unlike Member States, EU agencies and units must rely on various 'deliverables' coming from Member States' national intelligence authorities and international organisations, and gathered from freely accessible sources.

Examining intelligence tradecraft in the EU intelligence community is a challenging and onerous task. Diverse, often dispersed, sources of information and data, cross-cut competences of intelligence originators, discontinuities in the intelligence process, complex legal regulations and—last but not least—divergent attitudes to intelligence tradecraft on the part of EU institutions as well as Member States make for a broad yet incoherent background to the management, processing and sharing of strategic intelligence in the EU. For a long time intelligence objectives, needs and methods have been driven by the national interests of Member States, state security strategies and policies, and particular forms of intelligence tradecraft or *modi operandi*. A whole spectrum of tasks assigned to national intelligence agencies could not be performed at the European level, due to their sensitivity, relevance, organisational singularity and political peculiarity.

Against all these unpleasant determinants, Member States have gradually achieved considerable progress in the realm of common intelligence techniques, skills, organisational arrangements and pragmatic solutions. There are, however, some fields in which success has been fairly modest. Human intelligence, broadly understood (HUMINT), as well as electronic (ELINT) and signals intelligence (SIGINT) have simply been excluded from the scope of competence of EU agencies and bodies. However, certain areas of criminal intelligence, early warning, threat assessment, intelligence-led law enforcement and situational assessment of territorial security have gradually been incorporated as part of EU cooperation, particularly in the field of EU justice and home affairs.

This chapter elaborates on the basic conceptual elements of intelligence tradecraft, refers to EU practices and experiences in this regard, highlights the peculiarities of the EU approach and emphasises the protection of classified information.

The Notion of Intelligence Tradecraft

In the study of intelligence, the notion of 'tradecraft' describes the way in which intelligence becomes a commodity exchanged between agencies in order to gain a competitive advantage. A strict definition of 'tradecraft' is 'the techniques of the espionage trade, or the methods by which an agency involved in espionage conducts its business' (Lemer and Lemer 2004, p. 167). Tradecraft may also be conceived of as a skill set necessary for acquiring information and converting it into intelligence. Its fundamentals are relatively easy to learn because they reflect many years of experience, codes of conduct common to intelligence services throughout the world, organisational schemes and general security procedures.

The glossary of terms appended to one of the most valuable books on intelligence analysis (George and Bruce 2008, p. 309) describes intelligence tradecraft in the following way: 'Analytical tradecraft is the term used to describe the principles and tools used by analysts to instill rigor 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.' With regard to intelligence 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' (George and Bruce 2008, p. 319).

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, p. 167). Nowadays the craft of intelligence has to take into account the change in the targets of intelligence: from states (mostly global and regional powers) and international governmental organisations to non-state actors, terrorist organisations and transnational criminal networks (Treverton 2009, pp. 15–16). In the face of present-day problems, challenges and threats, tradecraft seeks to combine the 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 intuition with norms, procedures, guidelines, methods, organisational structures and—last but not least—technical and financial capabilities. The two dimensions of tradecraft, subjective and objective, correspond with the division into its operational and analytical aspects. The operational aspect emphasises practical skills and abilities in the conversion of available information and data into tactical intelligence, and the translation of intelligence products into operational support material. The analytical refers to the ability to process raw information and available data according to strategic guidelines and generalisations that will support and stimulate the performance of intelligence services.

Intelligence analysis is the core of tradecraft. Analytical tradecraft is the term used to describe the principles and tools used by analysts to instil rigour into their thinking and prevent cognitive biases from skewing their analytical judgments. Put simply, analytical tradecraft means 'the way analysts think, research, evaluate evidence, write, and communicate' (Department of Defense 2007, p. 312). Through the use of structured analytical 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 organise data, interpret their meaning, and produce judgments, insights and forecasts for policy makers and other users of finished intelligence products (Heuer 1981, pp. 297–8; Directorate of Intelligence 1997, pp. 25–7). Analytical performance is an indicator, a sort of litmus test, for the whole intelligence community as the provider of insights, and anticipatory and preventive guidelines. When effective and successful, it consolidates analytical tradecraft, validates the intelligence cycle and legitimises the entire analytic 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 2005a, p. 18).

The focus on the analysis and production of intelligence has overtaken the traditional feature of intelligence tradecraft as the set of methods, skills and instruments implemented in operations, rather than analytical work (Johnston 2005a, p. 17). However, recent changes in intelligence theory and practice suggest the increasing role of analytical aspects and the cognitive abilities of individuals participating in the intelligence cycle. 'Software' rather than 'hardware' predominates nowadays in the craft of intelligence. Recent failures prove that an intelligence community awash with data acquired by intelligence machinery risks overload and pressure from customers awaiting tailor-made solutions to identified security dilemmas.

Eminent intelligence scholars were asserting as early as 2008 that the future orientation of intelligence tradecraft would be an analysis-centric rather than collection-centric one (Treverton and Gabbard 2008, p. 44). However, there should be a good balance as well as synergetic connections between the two approaches. This is a demanding task for governments, national intelligence communities, and transnational institutions and agencies. The case of the European Union is no exception.

Categorising Intelligence

At every stage of the intelligence cycle, tradecraft has to take into account the functions, sources and means of intelligence. This is important for technical and organisational reasons, since every discipline requires specific elements of the craft of intelligence and delivers specific input to the cycle of intelligence analysis.

Intelligence activities can be grouped into four sectors:

1. Security intelligence is related to fundamental, constitutional bases of political governance and public order and is focused on domestic threats to the state, society and economy. It protects sovereignty, national interests, public order and social values against radical and extremist activities, subversion, espionage and terrorism.
2. Foreign intelligence is conducted overseas and consists in collecting information on the capabilities, intentions, objectives and activities of foreign actors: states, social groups and movements, economic entities. It serves foreign policy and diplomacy, delivering products which help to optimise decision making.
3. Military intelligence is focused on the actual and potential activities of the military forces observed within the territory of a given state or outside its borders. It is often used to support military missions and operations and facilitate the management of post-conflict stabilisation processes. It is conducted on tactical and operational levels where crisis management and combat missions are concerned. It is also deployed to strengthen prevention or to deal with the most serious threats to national interests, sovereignty and defence.
4. Criminal intelligence is concerned with the prevention and combating of serious and organised crime, which often has a transnational

dimension. It is drawn from information compiled, analysed and disseminated with the purpose of anticipating or preventing criminal activities, or carrying out surveillance operations. It can also provide law-enforcement services with an understanding of crime patterns and trends. It is often involved in criminal proceedings, enabling the acquisition of information in the pre-trial investigation phase. It is thus a means of gathering evidence and delivering it to the relevant judicial authorities.

These sectors can be grouped into certain categories: soft and hard intelligence depending on how the information is acquired; and human-driven and technology-driven intelligence depending on the role of the human factor.

1. Soft intelligence uses information and data provided voluntarily or on request, left open or made available from personal sources. Information also can be extracted from open sources, social media, diplomatic reports or public registers. Coercion, intimidation or any other form of pressure exerted on persons or groups to obtain specific information have no part in soft intelligence.
2. Hard intelligence is focused on secret or classified information. Interference in or disruption of the source of information, often in the wake of covert action, is used to overcome protective measures adopted by the source against unauthorised access. Hard intelligence is performed by highly skilled and well trained agents against critical personal targets. It can also employ sophisticated large-scale technical intelligence machinery, which enables the penetration of information systems, the invasion of data banks or the interception of encrypted communication.
3. Human-driven intelligence relies on individual abilities, skills and personal knowledge, used in close connection with information sources. It depends on human-to-human interface, but does not require direct interaction. Human intelligence is a classical form, although recently the significance of social media intelligence and open-source intelligence has increased since both disciplines explore sensitive and personal data provided by individuals and groups, physical and legal persons.
4. Technology-driven intelligence exploits the technical capabilities offered by technologies and solutions invented and developed in

> state laboratories and research institutions. Devices, appliances and hardware components using these technologies can acquire a massive quantity of standardised data. Technology-driven intelligence depends greatly on the application of devices and software to the collection, filtering and processing of large quantities of data, or the acquisition, transmission and storage of information extracted from classified, protected or hardly accessible sources.

A typology most frequently presented in the subject literature categorises sources of intelligence according to the type of information and data which is accessed, intercepted and collected by services or entities. The collection disciplines range from traditional tradecraft practised by spies and secret agents, through technically driven systems focused on information collection and processing to wide-ranging collection and analysis activity based on openly available sources. It should be added that technological changes as well as societal and cultural transformations have given rise to novel disciplines, exploring information and data amassed in social media, big-data storage solutions and—more generally—existing in cyberspace. Intelligence tradecraft tends to involve as many collection disciplines as possible, and each of the disciplines has strengths and weaknesses. As Lowenthal (2008, p. 19) points out, 'this should allow the collectors to gain advantages from mutual reinforcement and from individual capabilities that can compensate for shortcomings in the others'.

Human intelligence (HUMINT) relies on well-placed interpersonal contacts, be they open or covert, conducive to accessing certain information in the possession of a person or a group of persons (Richelson 1997, 1999, pp. 416–9; Shulsky and Schmitt 2002, pp. 11–22; Hitz 2007; Crous 2009; Johnson 2010, pp. 308–9; Rubin Peled and Dror 2010, pp. 321–3).

Protected information intelligence (PROTINT) explores the big data acquired by private and public institutions according to their legal competencies and tasks and related to the areas of their official activities (Omand 2000, p. 32; Gill and Phythian 2012, p. 80).

Signals intelligence (SIGINT) involves the remote acquisition and transmission of information and data through technologically advanced high-capacity electronic devices (Richelson 1999, pp. 406–12; Shulsky and Schmitt 2002, p. 27; Aid 2003).

Geospatial intelligence (GEOINT) means the exploitation and analysis of imagery and geospatial data to 'describe, assess, and visually depict physical features and geographically referenced activities on the Earth' (EUSC 2014a). It consists of imagery, imagery intelligence and geospatial information (Barrowman 2007, pp. 14–15). Imagery intelligence (IMINT) consists in obtaining information via satellite or aerial reconnaissance and the processing of pictures and other types of image (Shulsky and Schmitt 2002, pp. 22–7; McAuley 2005).

Measurement and signature intelligence (MASINT) analyses the physical attributes of certain objects, or targets, facilitating subsequent identification of and/or measurement of these objects (Shulsky and Schmitt 2002, pp. 31–2; Clark 2007, pp. 44–5).

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, unclassified government publications and publicly available data (Hulnick 2002; Politi 2003; Mercado 2005; Steele 2007; Antoniou 2013; Hobbs et al. 2014; Olcott 2014).

In addition to the above-mentioned traditional intelligence collection disciplines, new variants have appeared recently, highlighting the changing nature of today's infosphere, the rapid and massive expansion of information sources and emerging challenges to the intelligence community. These new collection methods reflect the variation in cultural environments as well as the expanding application of technologies to intelligence processes. Moreover, the state, with powerful, expensive machinery enabling large-scale surveillance and data retention, probably remains the predominant actor in intelligence acquisition and collection. The Snowden affair disclosed the magnitude of the US administration's efforts to amass intercepted information and data. Nevertheless, private companies and independent entities, including NGOs, can conduct impressive intelligence work without HUMINT or SIGINT collection capabilities. Instead, they explore publicly available sources, social media or Internet resources. They invent and deploy new tools to harvest data from all over the Internet for both business and strategic intelligence purposes.

The following are some examples of non-traditional intelligence collection disciplines which are rapidly becoming popular.

Social media intelligence (SOCMINT) is a relatively new discipline responding to the rapid virtualisation 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 (Appel 2011, pp. 24–8; Liaropoulos 2013; Tzanetti 2013; Omand et al. 2012, 2014).

Socio-cultural intelligence (SOCINT) was developed as a result of the growing importance of information about the social and cultural environment obtained and analysed in countries in which diplomatic missions were present. SOCINT seeks, according to Sorentino (2011), 'to understand the why factor as it applies to their behavior and how that behavior is being driven by their mindsets, perceptions, beliefs, customs, ideologies and religious influences'. Patton argues that 'Incorporating the sociocultural information provides situational understanding and predictability in anticipating overpressure or second and third order of effects possibilities' (Patton 2010, p. 14. Also Richelson 2012; Gill and Phythian 2012, pp. 79–81; Phythian 2013b, pp. 2–3).

Research-originating intelligence (RESINT) is another conceptual attempt to respond properly to the dynamically changing properties of global information flows, data overload, the digital tsunami and other features of today's infosphere. RESINT is largely based on open sources. It can facilitate all-source analysis due to its ability to cross-reference to other information sources and disciplines of intelligence collection, including clandestine and covert sources (Svendsen 2013).

Cyber intelligence (CYBERINT) emerges within cyberspace, a domain encompassing physical elements of computing and information infrastructure as well as computer programmes and applications which give birth to virtual 'parallel' worlds imitating real-world elements and structures. Cyberspace is not only a realm allowing for relatively free, quick and extensive communication; it also contains interconnected virtual organisations, networks and systems regulating, controlling and steering ever-growing areas of public activity (Inkster 2010, pp. 55–6; INSA 2011; Braganca 2013). CYBERINT can be defined as a set of activities which aim at 'obtaining prior knowledge of threats and vulnerabilities to information communications systems through a variety of technical means' (Brantly 2013, p. 79).

Situational intelligence (SITINT) originally applied to business intelligence solutions yet over time it has widened the scope of its application. Now SITINT 'combines traditional situational awareness with the collective intelligence of those at the center of a situation, resulting in a dynamic process in which data is gathered and interpreted and the information is shared' (Dent 2013). SITINT solutions combine data gathering, correlation and analysis, visualisation and display (Space-Time Insight 2014, pp. 7–8). They enable the vertical structuring of high volumes of disparate data, encompassing geographically distributed information, real-time operational data, open-source news (RSS feeds, statistics, weather forecasts), mobile applications (social media posts, photos and movies, field reports, emergency alerts). This intelligence discipline puts greater emphasis on situational factors, as they are susceptible to change or fluctuation and require a good sense of control (Hayward 2007, p. 235; BPM Partners 2010). Analytical models and tools used in SITINT tradecraft are equipped with alert functions and preventive solutions but they are focused on improving the effectiveness of decision making in ongoing operations.

The above taxonomies have been presented to strengthen the argument for selectivity in EU intelligence tradecraft, and to illustrate its relationship to a traditional typology of intelligence disciplines. Next, EU intelligence cooperation activities will be discussed in relation to the above-listed disciplines, focusing on source collection. A wider spectrum of intelligence systems will be presented in the following chapters.

As an international organisation *sui generis*, the EU does not include every discipline in its intelligence tradecraft. This also reflects the argument developed throughout this book that the European Union builds its intelligence community on the strategic level. The strategic requirements of EU security policies put certain restrictions on EU activities in certain intelligence disciplines. The political rationale behind intelligence cooperation at the Union level precludes EU institutions or agencies from developing a comprehensive all-discipline system. Technical and financial factors also effectively hinder progress in technical and scientific areas, especially signals intelligence and surveillance.

Selected Intelligence Disciplines in EU Tradecraft

Although the EU intelligence community aims to develop its activities in every one of the intelligence disciplines, its efforts are unevenly distributed and its competences largely depend on Member States. Unlike national intelligence communities, the European Union has to combine and integrate institutions, measures, tools and procedures belonging to different legal and institutional orders. Certain constraints originate in national determinants: geopolitical location, legal tradition, strategic culture, political system, economic position. Others emerge due to specific restrictions imposed on EU institutions and agencies by Member States, EU law or inter-agency regulations. In general, the legal and institutional separation of external and internal security policies makes intelligence cooperation more complicated and heterogeneous.

The strategic level of EU intelligence cooperation determines which disciplines appear only to a limited extent, and which are treated as a priority. The EU prefers soft intelligence measures and displays rather more caution towards advanced invasive technical intelligence (TECHINT) elements. The production of hard intelligence by EU agencies or services is effectively forbidden. It is only permitted to reach EU level from Member States, when it is subject to political agreements, operational planning, emergency procedures and individual decisions. Moreover, it should be properly secured, classified and protected against any distortion or misuse. Soft intelligence clearly prevails in EU intelligence tradecraft. EU agencies and bodies are fed with plenty of information collected, pre-processed and transmitted by various institutions and services representing Member States and many non-EU partner states and organisations. Similarly, open-source information and publicly available data are acquired and processed within the intelligence cycle.

Human Intelligence

The European Union does not use human intelligence as such, with the important exception of its military intelligence cooperation (see Chap. 4). It relies on input from the national intelligence agencies and law-enforcement services. Statements by representatives of the European Commission asserting that the EU has no plans to establish a secret intelligence agency can be interpreted as a firm declaration precluding the possibility of working out autonomous intelligence capabilities based on HUMINT and SIGINT. However, members of EU missions abroad under the CSDP may incidentally collect information from local sources.[1]

There are occasions when tentative actions undertaken by EU intelligence staff have immediately been declared by high-ranking EU officials to not be genuinely ‘intelligence driven’ but to be part of the ordinary activities of the relevant EU institutions. This was the case with the EEAS missions to Libya in March and April 2011. When the media reported on the presence of SITCEN staff in the fact-finding team sent to Tripoli and Benghazi, Ilkka Salmi, the head of SITCEN, confirmed the reports but underlined the fact that two persons sent to Libya with the EEAS team were ‘technical specialists who went to help with satellite phones and that type of thing’ (Rettman 2011). He underscored the non-operational character of their roles, asserting that ‘there was certainly no tasking’, that SITCEN ‘does not hunt for its own information’ and that it was focused on strategic issues rather than operational intelligence (Rettman 2011). Interviewed in

March 2014, Salmi reiterated his comment that the presence of SITCEN staff in Libya was ‘never any type of intelligence operation’, stressing that the EU Intelligence Analysis Centre (formerly SITCEN) ‘do[es] not have any intelligence officers anywhere around the world. No operations’ (Clerix 2014). Likewise, it was noted during the refugee crisis in 2015 that Frontex, an agency responsible for risk management and situation assessment, did not dispatch a single official to gather intelligence in the border areas witnessing migrant pressure (Mathiason et al. 2015). ‘Soft’ elements of HUMINT tradecraft may, however, be found in socio-cultural intelligence, which is described below.

Protected Information Intelligence

PROTINT explores big data acquired by private and public institutions in accordance with their legal competencies and tasks and related to the areas of their official activities. In this context, protected information is ‘personal information about individual that resides in databases, such as advance passenger information, airline bookings and other travel data, passport and biometric data, immigration, identity and border records, criminal records, and other governmental and private sector data, including financial and telephone and other communications records’ (Omand 2000, p. 32). This information is protected by law, mostly due to its personal nature and privacy issues, yet it is available to relevant state authorities and is sometimes subject to international exchange on the basis of appropriate agreements. Its value grows with the scale of data mining in data sets and data-bank systems, or ‘warehouses’, and the ability of analysts to link large quantities of information in order to extract interesting patterns or dependencies. Intelligence services can access these warehouses without formal warrants, yet they cannot influence the way information is collected, stored and made available by the respective institutions (Gill and Phythian 2012, p. 80).

EU databases collect and store large amounts of information, mainly personal data, related to internal security and external threats (terrorism, organised crime, illegal migration). In general terms, the data stored in EU information systems can be exchanged among the agencies and bodies holding the databases or transferred to third parties with which the relevant EU institution or agency has concluded an exchange agreement. In practice, data acquired and stored by EU agencies operating in the area of freedom, security and justice (AFSJ), such as Europol, Frontex and Eurojust, as well as OLAF (the European anti-fraud office), are associated with large-scale information systems established with the purpose of securing the free movement of persons within the EU and the Schengen zone as well as regulating immigration and asylum issues in the political and legal framework of the EU. These systems, such as the Schengen Information System (SIS), the Visa Information System (VIS), the Customs Information System (CIS) or Eurodac (the European fingerprint database), gather personal data as well as information about objects relevant to internal security or criminal justice (Boehm 2012). Much of the information stored in these systems is concerned with serious security threats or sources of risk to EU security, stability and public order.

The rapidly increasing amount of data stored in large-scale IT systems opens up additional channels for EU agencies when searching for a piece of given information, checking data against stored files or linking same-category data kept in separate warehouses. Such practices affect the original aims behind the large-scale centralised information systems, like the SIS, which were established to ensure the proper functioning of the area of free movement of persons and not as a tool for the prevention and combating of transnational organised crime or terrorism.

Socio-cultural Intelligence

Lessons learnt by politicians, the military and scholars when managing, resolving or studying conflicts in the Balkans, the Middle East, the Horn of Africa, the Persian Gulf, North Africa and—last but not least—the AfPak area, evidence the growing relevance of cultural and religious determinants as well as social and psychological factors. The routine collection of information from traditional sources has come back into favour, highlighting the relevance of socio-cultural factors to situational awareness, risk assessment and threat profiling.

The European Union has developed SOCINT capabilities in the framework of the CFSP and the external dimension of its activities. The European Union maintains diplomatic missions throughout the world. Representing the EU in almost 140 countries and international organisations, the European Commission delegations make up the core part of the European External Action Service (EEAS), established in 2010 under the Lisbon treaty. Moreover, EU Special Representatives have been assigned to specific regions and crisis areas, such as the Balkans, the Southern Caucasus, the Great Lakes region and the Horn of Africa and for the

Middle East peace process. Special envoys, fact-finding teams and EU civilian and military mission personnel are able to openly collect information from a wide range of sources. Local contacts are most valuable; they may even occasionally provide confidential information, share detailed knowledge of specific issues and give hints as to understanding better certain structurally embedded social, cultural or political traits (Walsh 2006, p. 636). Although the diplomatic status of EU delegates and officials forbids them to engage in systematic data collection or analysis of intelligence, information gathered, acquired or 'dug up' in situ may quite often propel intelligence analysis and thereby contribute to decision-making processes at the EU institutional level.

Geospatial Intelligence

Contemporary military operations or expeditionary missions (civilian, humanitarian, rescue, etc.) cannot be properly conducted without the building of a situational awareness encompassing surveillance, monitoring and forecast in the planning, command and control phase as well as in the follow-up to the operations and missions.

A capacity to use satellite imagery for security purposes was discussed by EC Member States as early as the beginning of the 1990s, before the EU was constituted. The lessons learnt in the Persian Gulf and the Balkans clearly indicated the weaknesses of crisis-management mechanisms and humanitarian missions performed by the EC's members under the aegis of the Western European Union (WEU). The deficit of intelligence capabilities, especially in the field of geospatial information and knowledge, was acknowledged by the major actors in European security. They decided to set up within the WEU a small unit called the Satellite Centre (SATCEN). SATCEN was inaugurated in April 1993 and tasked with compiling and processing accessible imagery data and making them available to WEU Member States, particularly for the purposes of arms-control agreements, crisis monitoring and environmental monitoring (WEU 1994).

With the creation of the European Security and Defence Policy (ESDP) and the establishment of its institutions, SATCEN was transferred in 2002 to the European Union, incorporating the relevant features of the existing WEU structures. Since the Lisbon treaty reform and legal changes, SATCEN has been an agency that supports the decision making of the European Union in the field of the CFSP, and in particular of the ESDP, by providing products of satellite imagery analysis and collateral data, including aerial imagery, and related services (Council of the EU 2001c). It operates under the political supervision of the Political and Security Committee (PSC) and operational direction of the High Representative for the CFSP. At the request of various users it provides geospatial intelligence, satellite imagery analyses, topographic surveys, cartographic maps and briefing notes for the purposes of situational awareness, early warning and crisis monitoring, rapid response requirements, generic and contingency planning by EU missions and operations, and general security surveillance.

Since SATCEN does not have access to satellite sensors, the primary sources of satellite data are commercial providers activated on a case-by-case basis. (European Parliament 2010c). EU Member States having repeatedly expressed a need for the autonomisation of the CSDP, SATCEN has directed its efforts towards a wider use of EU space assets contributed by several Member States (Germany, France, Italy, Spain, Belgium, Greece) (EUSC 2013).

Apart from imagery analysis and geospatial intelligence, SATCEN also acquires and processes collateral materials derived from open sources and government files containing, for instance, aerial imagery, analytical reports or on-site data.

Cyber Intelligence

Like any public domain, cyberspace is vulnerable to threats, attacks and malicious actions from different actors having various motivations, intentions, goals and tools. Cyberspace security has become a growing challenge and a real problem for governments, public authorities, private and public companies and—last but not least—individual users. The interconnectivity of users, or the 'systems of systems' architecture, creates security problems which must be tackled by knowledgeable professional institutions and services in order to prevent damage, protect information sources and databases, and safeguard critical elements of public infrastructure. Cyber espionage, intrusions and attacks on data banks have become everyday features of global communication networks.

Since the late 1990s, the European Union has developed a comprehensive strategy for electronic network and IT systems security, including the practical implementation of actions containing some elements of cyber intelligence. In 2004 the European Union Agency for Network and Information Security (ENISA) was established 'to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via [information] networks and systems' (European Parliament and the Council 2013a, p. 48). It was decided that the agency should assist the Union and Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents. ENISA's tasks include the collection, processing and analysis of data and the dissemination of information and reports on IT security incidents in the EU, as well as on emerging risks and security threats. ENISA has developed a conceptual framework for the analysis and reporting of emerging and future risks in the area of network information security (ENISA 2010, p. 5).

Recently CYBERINT has become one of the priority domains in Europol's activities. With the expansion of virtual networks and global communication, Europol decided to intensify its involvement in the building of cyber-security resilience and capacity to handle the growing problem of cyber-criminality. In 2009 it established, on the initiative of the French presidency in 2008, a European CyberCrime Platform to coordinate Member States' responses to cross-border Internet-related criminal phenomena (House of Lords 2010, pp. 124–5; Hillebrand 2010). These efforts culminated in 2013 with the establishment of the European Cybercrime Centre (EC3) (House of Lords 2010, pp. 124–5; RAND 2012, p. 87). The centre is focused on data fusion: collating information on cybercrime delivered by Member States and gathered from open sources. It also processes and analyses information and pre-produced intelligence for the purpose of delivering threat assessments. According to information on the official EC3 website, the Centre 'acts as an analytical hub, processing and analysing critical information from various sources on an ongoing basis. The goal is to broaden the information picture on cybercrime in Europe over time so as to rapidly identify emerging threats' (European Cybercrime Centre 2014).

Open-source Intelligence

EU agencies and entities involved in intelligence cooperation increasingly use open sources in their everyday activities. Although the difference between a military intelligence hub, criminal intelligence hub or diplomatic hub is obvious in terms of the scope, intensity, usability and reliability of the open sources they use for their specific purposes, the influence of OSINT has undoubtedly continued to grow. This is also connected to the very nature of EU intelligence tradecraft: the scarcity of classified, top-secret or highly sensitive information in the possession of EU bodies needs to be balanced by open-source information acquired beyond Member States' strict and—quite often—highly demanding requirements. Hence, OSINT is 'doomed' to being the intelligence discipline that allows for the avoidance of national restrictions, limitations and blockades on secret information.

Open-source intelligence was the predominant mode of activities conducted by SITCEN, now the EU Intelligence Analysis Centre (INTCEN). Given that the sharing of very sensitive information was forbidden, SITCEN collected preselected information delivered voluntarily by Member States. The contents were analysed and draft reports or situation assessments were prepared, subject to further examination. Open-source information was therefore collated and—if possible—related to fragmentary material obtained from Member States. In the mid-2000s, following terrorist attacks on European soil (Madrid and London) and the escalation of violence in local and regional conflicts in Africa and Asia, SITCEN began developing an enhanced OSINT capability in support of strategic intelligence at EU level (House of Lords 2009, p. 32).

Open sources are also important for EU agencies located in the criminal intelligence hub. Although both Europol and Eurojust, as well as Frontex, are in a better position than INTCEN or the EU Military Staff (EUMS) Intelligence Directorate, with regard to the level and intensity of national intelligence inputs, they are happy to access publicly available information. Open-source data are systematically monitored, collected and processed. They underpin the description and analysis of the situation outside the EU. They are also used as a supplementary asset for horizon scanning in the crime environment (Europol 2008, pp. 8–9; 2013, p. 43).

Open-source intelligence has also been practised by Frontex in data-collection and risk-analysis undertakings. Frontex's strategic intelligence, situational awareness and risk analysis are reinforced considerably by open-source information and data. In its 2012 annual risk analysis, Frontex declared that: 'Open sources of information were also effectively exploited, especially in identifying the main push and pull factors for irregular migration to the EU. Among others, these sources included reports issued by government agencies, international or non-governmental organisations, as well as official EU reports, such as the Commission's reports on third countries, and mainstream news agencies' (Frontex 2012, p. 7).

All-Source Analysis

National intelligence organisations tend to develop all-source analysis, fusing all available information for the purposes of collating it, processing it and producing intelligence. All-source information consists in the evaluation, interpretation and assessment of information extracted from a wide variety of sources, both overt and covert (Herman 1996, p. 100; Russell 2007b). Despite the evident limitations of information exchange and intelligence sharing in the EU, the need for the strategic integration of dispersed information has been articulated on several occasions by EU officials. Gilles de Kerchove, EU Counter-Terrorism Coordinator, in a short introduction to a report on fusion centres in Europe, argued that: 'The SITCEN has developed into a unique platform where strategic intelligence produced by the intelligence, security and military services, police information collected by EUROPOL and open sources are integrated and summarised' (de Kerchove 2010, p. xxi). In a similar vein, Johnny Engell-Hansen, the former head of the Operations Unit at SITCEN said the following in 2009: 'Essentially, we are now able to fuse open sources information, diplomatic reporting, military and civilian intelligence into all-sources situation assessments' (House of Lords 2009, p. 32).

All-source analysis has been practised more or less successfully by sectoral units responsible for the established security field: INTCEN for military and civilian security, and Europol for internal security. INTCEN's strategic intelligence is built on all-source analysis although this does not entail the use of raw intelligence and operational information held by Member States. Thus, INTCEN has to collate and analyse pre-processed or secondary information made available by public or private sources or acquired from large-scale communication networks (Nomikos 2014, pp. 7–8).

Europol also tends to apply an all-source analysis to the production of strategic intelligence threat assessments and situational reports. It takes advantage of information and data delivered by national law-enforcement and/or internal security agencies from Member States and, if necessary, third countries and organisations and stored in Europol's files and databases. EU agencies and bodies like INTCEN, Eurojust and the office of the EU Counter-Terrorism Coordinator can also contribute relevant data. Europol collates these data with information mining from public media and other open sources, like government documents, academic publications or so-called grey literature.

All-source analysis within the intelligence community is still the EU's frame of reference. However, too many loopholes in the intelligence workflow hinder the proper use of sources and materials available to EU actors. Some attempts have been made to integrate dispersed sources and enhance national inputs to the intelligence process unfolding in certain fields of EU security policy. The strategic intelligence level especially looks set to see an expanding flow of information and data originating in varied sources of EU intelligence cooperation.

The Intelligence Process in the EU

The specific character of the EU intelligence community is manifested in the variety of intelligence tradecraft elements producing different effects at various stages and levels of cooperation. The multitude of actors, norms, practices, means and goals does not help the adoption of a unified approach and the working out of a comprehensive approach to the intelligence cycle. The dynamic of integration processes in the EU is also influenced by the attitudes of relevant national and supranational actors towards intelligence tradecraft.

In the late 1990s/early2000s, the predominant approach to the intelligence cycle in the EU was determined by four factors: first, attachment to the classical notion and conceptualisation of the intelligence cycle; second, the clear and deep division between the internal (law-enforcement) and external (military) dimensions of EU security policy; third, the low levels of EU intelligence cooperation; and fourth, the overwhelming influence of certain Member States' experiences of patterns, practices and solutions of information exchange and intelligence sharing. It is significant that intelligence cooperation unfolding in the two main dimensions of EU security—the internal and the external—was at that time framed in the traditional intelligence cycle model.

Björn Müller-Wille described the intelligence cycle with regard to security and defence policy as a sequential step-by-step process evolving in five stages: collection, processing, analysis, dissemination and task/control. He emphasised the scarcity of technical, professional and personal resources and assets at EU level, as well as the organisational diffusion that weakens analysis capacity (Müller-Wille 2002, pp. 66–77). Despite the unquestionable achievements of the CSDP, the intelligence cycle did not abandon the specific vertical configuration which made information flow dependent on input from Member States. National defence intelligence agencies have been the main source of relevant data, providing crucial input to intelligence analysis at EU level. Therefore, the intelligence requirements set by relevant EU bodies, mainly the Intelligence Directorate of the EU Military Staff (EUMS INT) and INTCEN, have to correspond to national intelligence rules and mechanisms of information sharing. This is particularly important in the collection phase due to the fact that national services can employ much more diversified forms, means and methods than EU units. As a result, national intelligence organisations can use HUMINT and SIGINT to dig up and collect sensitive information and data, yet they are not obliged to share them with EU bodies or other Member States. Even if military intelligence services provide information and data to the EUMS INT, the 'ownership' of intelligence is a factor regulating further circulation of a given file. The delivering state may limit access to the file on the need-to-know principle, or based on the aim of supplying it.

Analysis is largely the domain of INTCEN. The Centre works on open-source material, military and non-military intelligence from several Member States and diplomatic reports. Its specialists use open-source data or cross-check available national reports or other intelligence deliverables to produce their contextual analysis. INTCEN's main intelligence products are situation and risk assessments built on all-source analysis and updated every six months, as well as special reports and briefings. INTCEN also prepares daily intelligence summaries containing a detailed description of important events or facts and in-depth analysis based on available intelligence and data (INTCEN 2015). In the final stage, intelligence products are distributed to authorised customers. The High Representative for Foreign Affairs and Security Policy/Vice-President of the European Commission is the primary recipient along with the senior management of the EEAS. Strategic assessments are delivered to several Directorates-General of the Commission and to the Council's General Secretariat. The reports are also shared with the governments and intelligence services of Member States.

While matters of military security and defence corresponded with the vertically oriented information delivery and processing chain, internal security and law enforcement preferred horizontal arrangements, allowing more collation and cross-referencing among EU-based entities involved in intelligence activities. Nevertheless, the logic of the classical intelligence cycle predominated in early efforts to introduce and complete a full cycle of information management and intelligence production. The European Police Office is a particularly telling example. Jürgen Storbeck, the first director of Europol, outlined a cycle suitable for this unit in its early stages, when open sources prevailed over classified information delivered by Member States. This cycle consisted of five steps: planning and direction; collection; processing; production; and dissemination and evaluation (Storbeck 1999, pp. 6–7).

When Europol began its fully fledged activities, the need to provide knowledge about intelligence analysis techniques and capabilities resulted in analytical guidelines elaborated by Europol's Analysis Unit within the Intelligence Model Framework. These guidelines contained a detailed description of 'the intelligence process' which partially departed from the previous cyclical approach and put greater emphasis on linkages and cross-references between the parts of the process. The intelligence process comprised typical elements of the intelligence cycle: collection, evaluation, collation, analysis and dissemination of intelligence. However, these activities required substantial advance planning and a comprehensive assessment on the basis of available information and knowledge. The chain of information management had its beginning in requirements, priorities and objectives which determine the scope and character of tasking. The analysis stage is crucial because it links to collection and can thus streamline information gathering, yet it also has a direct impact on the identification of further objectives and the launching of more general projects. The latter are closely related to the priorities and general requirements of the intelligence process.

The framing of law-enforcement cooperation within the European Criminal Intelligence Model (ECIM) stimulated modifications in Europol's intelligence process. The creation and implementation, from 2010 on, of an EU-wide policy cycle for organised and serious international crime was a considerable step forward. The new methodology of criminal intelligence contained in the Serious and Organised Crime Threat Assessment (SOCTA), adopted in 2012, proceeds from the identification of focal areas which are also a starting point for data collection. These areas are monitored with the use of certain methods and tools, such as tailored indicators, relevant factors and horizon scanning. The data needed for SOCTA are extracted from Europol's available databases, especially from appropriate analysis work files. Additional information comes from Europol's analytical and intelligence products, such as specific threat assessments and strategic reports as well as threat notices and profiles of new and emerging trends drawn from Europol's SCAN (scanning, analysis and notification) system (Europol 2010). OSINT supplements the scanning of the crime environment. The identification of intelligence gaps as a result of the preliminary analysis enables the development of tailored EU intelligence requirements which are distributed to various stakeholders in questionnaires requesting descriptive data for the threat indicators, and information about new or emerging trends (Council of the EU 2012b, pp. 17–18).

Europol tends to apply an all-source analysis: information delivered by Member States and requested from third countries and organisations is collated with open-source material, especially reports from public organisations and the private sector, scientific reports and publications, EU and other official documentation as well as journals, magazines, news agency reports and newspapers. In case of contradictions or ambiguities, information extracted from OSINT is cross-checked with the Member States involved. In the analysis phase, the data are processed and the indicators assessed with reference to key threats, both current and future. The results of the intelligence process are integrated with the policy cycle for organised and serious international crime. They contain a list of recommended priorities, argument maps and inputs for the preparation of multi-annual strategic plans in a later phase of the policy cycle (Council of the EU 2012b, p. 25).

The intelligence processes occurring within the EU intelligence community are clearly heterogeneous. This is an intrinsic feature of any transnational intelligence cooperation. Nevertheless, it is worth underlining the fact that Member States and relevant EU institutions and agencies have sought to implement mechanisms and solutions optimising the information workflow and enhancing analytical capabilities at the EU level. Hitherto, the effects have been mixed. The most effective intelligence cycle has been adopted in the fields of criminal analysis and internal security governance. Despite numerous shortcomings and systemic barriers, it has brought about a cohesive and flexible framework for information sharing and intelligence cooperation among the host of stakeholders. As far as military intelligence is concerned, the intelligence process within the EU is, essentially, contested by Member States wary of security arrangements and safety regulations at the EU level.

Doing Intelligence in the EU: Concluding Remarks

Intelligence tradecraft in the EU intelligence community reflects the complex web of interdependencies connecting numerous participants who are willing to cooperate in information exchange and intelligence sharing. It follows that the methods, principles and tools used by intelligence actors vary greatly, especially when applied at the national level. The centre of gravity in the area of intelligence cooperation has been direct collaboration among national services, quite often outside the framework of the EU (Müller-Wille 2008, pp. 55–8). Member States are not bound to provide intelligence to other members or to EU institutions or agencies. However, a growing willingness to cooperate and deliver valuable inputs to EU data systems and information repositories has been clearly noticeable for some time. The increasing amount and diversity of information and intelligence transferred at the EU level have led to co-ordination of elements of intelligence tradecraft and attempts to frame an EU model of analytical tradecraft.

Intelligence-led solutions, analytical models and policy cycles are evidence of responses by competent EU institutions and agencies to stimuli from particular Member States seeking to improve the management of sensitive information and reliable data acquired by the components of the EU intelligence community. The intelligence process is still decentralised and subject to national predilections and habits, or national security cultures, which quite often restrict the scope of intelligence cooperation at EU level. However, both Member States and EU agencies and institutions seek to enhance their tradecraft capacities and skills through the delivery of valuable inputs, and relevant and profitable outcomes. This is crucial to the consolidation of a robust, effective and legitimate intelligence community in the EU. So far, intelligence products offered by EU agencies have been fairly useful but lack high credibility due to the restrictions imposed by individual Member States on the transmission of the sensitive information and raw material they possess. This may result from low confidence in EU-led methods, instruments and measures in the realm of strategic intelligence. But this scepticism does not necessarily correspond with the real capabilities of EU agencies and units.

In addition to the leading products, such as Europol's SOCTA and TE-SAT or Frontex's FRAN reports and ARA, there are numerous tailored analyses addressing specific requests by consumers, especially those concerning the anticipation, foreknowledge and prevention of 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 attempt to develop and widen the cognitive capabilities of the EU intelligence community.

Intelligence tradecraft has been characterised by the progressive adaptation and implementation of qualitative and quantitative methods of data analysis and information management by competent EU agencies and entities, most of all Europol, Frontex and INTCEN. Strategic intelligence is the area in which 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 EU strategic intelligence community.

Note

1. Anonymous EEAS official, interview October 2013.

Bibliography

Aid, M. M. (2003). All glory is fleeting: Sigint and the fight against international terrorism. *Intelligence and National Security, 18*(4), 72–120.

Antoniou, A. (2013). *Open source information. The future of intelligence*. Athens: European Intelligence Academy.

Appel, E. J. (2011). *Internet searches for vetting, investigations, and open-source intelligence*. Boca Raton: CRC Press.

Barrowman, R. A. (2007). Geospatial intelligence. The new intelligence discipline. *Joint Force Quarterly, 44*(1), 14–18.

Boehm, F. (2012). *Information sharing and data protection in the area of freedom, security and justice. Towards harmonised data protection principles for information exchange at EU-level*. Berlin/Heidelberg: Springer-Verlag.

BPM Partners (2010). Situational intelligence: The key to agile decision making. At http://www.salient.com/docs/BPM_Partners-Situational_Intelligence.pdf. Accessed 17 Apr 2014.

Braganca, M. (2013). Hunt for red October. The new face of cyber espionage. *SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis, 2*, 37–44.

Brantly, A. (2013). Defining the role of intelligence in cyber. A hybrid push and pull. In M. Phythian (Ed.), *Understanding the intleligence cycle*. London/New York: Routledge.

Clark, J. R. (2007). *Intelligence and national security: A reference handbook*. Westport/London: Praeger Security International.

Clerix, K. (2014). Ilkka Salmi, the EU's spymaster. *Mondiaal Nieuws*, 4 March. At http://www.mo.be/en/interview/ilkka-salmi-eu-s-007. Accessed 10 June 2014.

Council of the EU (2001c, July 25). Council joint action 2001/555/CFSP of 20 July 2001 on the establishment of a European Union Satellite Centre. *Official Journal of the European Communities, L 200*, 25.

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

Crous, C. (2009). Human intelligence sources: Challenges in policy development. *Security Challenges, 5*(3), 117–127.

Davies, B. (2005). *The Spycraft manual. The insider's guide to espionage techniques.* London: Carlton Books.

De Kerchove, G. (2010). Future challenges in the fight against terrorism. In Belgian Standing Intelligence Agencies Review Committee (Ed.), *Fusion centres throughout Europe. All-source threat assessments in the fight against terrorism*. Antwerp/Oxford/Portland: Intersentia.

Dent, C. (2013, July 12). Situational intelligence for effective decision making, critical communications. *Wired*. At http://www.wired.com/2013/07/situational-intelligence-for-effective-decision-making-critical-communications/. Accessed 17 Apr 2014.

Department of Defense (2007). The Silberman-Robb Commission recommendations on intelligence and WMDs in Iraq, 2005. In L. K. Johnson (Ed.), *Strategic intelligence* (Vol. 2). Westport/London: Praeger Security International.

Directorate of Intelligence (1997). *A compendium of analytic tradecraft notes.* Langley: Central Intelligence Agency. At http://www.oss.net/dynamaster/file_archive/040319/cb27cc09c84d056b66616b4da5c02a4d/OSS2000-01-23.pdf. Accessed 4 Dec 2012.

ENISA (2010). *EFR framework. Introductory manual.* At http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/emerging-and-future-risks-framework-introductory-manual/at_download/fullReport. Accessed 19 June 2012.

European Cybercrime Centre (2014). Services. At https://www.europol.europa.eu/ec3/services. Accessed 28 Sept 2014.

European Parliament (2010c, November 30). Reply to written question E-6003/2009by Martin Ehrenhauser (NI) to the Council. Subject: Work of the European Union Satellite Centre (EUSC). At http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2009-6003&language=EN. Accessed 8 Mar 2013.

European Parliament and the Council of the EU (2013a, June 18). Regulation (EU) no 526/2013 of the European Parliament and of The Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004. *Official Journal of the European Union, L 165.*

Europol. (2008). *EU terrorism situation and trend report 2008.* The Hague: Europol.

Europol (2010). Europol launches scan system for strategic notices on newly identified organised crime threats, 1 January. At https://www.europol.europa.eu/sites/default/files/publications/2010-oc-scan-threat-notice-open-version.pdf. Accessed 11 Jan 2010.

Europol. (2013). *SOCTA 2013. EU serious and organised crime threat assessment*. The Hague: European Police Office.

EUSC. (2013). *EU SatCen annual report 2012*. Luxembourg: Publications Office of the European Union.

EUSC (2014a). *Geospatial intelligence*. Madrid: EU Satellite Centre. At http://www.satcen.europa.eu/index.php?option=com_content&task=view&id=8&Itemid=16. Accessed 17 Mar 2015.

Frontex. (2012). *Annual risk analysis 2012*. Warsaw: Frontex.

George, R. Z., & Bruce, J. B. (Eds.). (2008). *Analyzing intelligence: Origins, obstacles, and innovations*. Washington, DC.: Georgetown University Press.

Gill, P., & Phythian, M. (2012). *Intelligence in an insecure world* (2nd ed.). Cambridge: Polity Press.

Hayward, K. (2007). Situational crime prevention and its discontents: Rational choice theory versus the culture of now. *Social Policy and Administration, 41*(3), 232–250.

Herman, M. (1996). *Intelligence power in peace and war*. Cambridge: Cambridge University Press.

Heuer, R. J., Jr. (1981). Strategic deception and counterdeception: A cognitive process approach. *International Studies Quarterly, 25*(2), 294–327.

Hillebrand, C. (2010, November 11). Fighting cyber crime. *Europe on the Strand*. At http://europeonthestrand.ideasoneurope.eu/2010/11/11/fighting-cyber-crime/. Accessed 7 Jan 2012.

Hitz, F.P. (2007). Human source intelligence. In L.K. Johnson (Ed.), *Handbook of intelligence studies*. London/New York: Routledge.

Hobbs, C., Moran, M., & Salisbury, D. (Eds.). (2014). *Open source intelligence in the twenty-first century. New approaches and opportunities*. Basingstoke/New York: Palgrave Macmillan.

House of Lords (2009). *Civil protection and crisis management in the European Union. Report with Evidence*. HL Paper 43. London: The Stationery Office.

House of Lords (2010). *Protecting Europe against large-scale cyber-attacks. Report with Evidence*. HL Paper no. 68. London: The Stationery Office.

Hulnick, A. S. (2002). The downside of open source intelligence. *International Journal of Intelligence and CounterIntelligence, 15*(4), 565–579.

Inkster, N. (2010). China in cyberspace. *Survival, 52*(4), 55–66.

INSA (2011). *Cyber intelligence. Setting the landscape for an emerging discipline*. INSA Cyber Intelligence White Paper. At https://images.magnetmail.net/images/clients/INSA/attach/INSA_CYBER_INTELLIGENCE_2011.pdf. Accessed 17 Apr 2014.

INTCEN (2015). *EU INTCEN fact sheet*. At http://eeas.europa.eu/factsheets/docs/20150206_factsheet_eu_intcen_en.pdf. Accessed 17 Apr 2015.

Johnson, L. K. (2010). Evaluating "Humint": The role of foreign agents in U.S. security. *Comparative Strategy, 29*(4), 308–332.

Lerner, K. L., & Lerner, B. W. (2004). Tradecraft. In K. L. Lerner & B. W. Lerner (Eds.), *Encyclopedia of espionage, intelligence, and security* (Vol. 3). Detroit: Thomson Gale.

Liaropoulos, A. N. (2013). The challenge of social media for the intelligence community. *Journal of Mediterranean and Balkan Intelligence, 1*(1), 5–14.

Lowenthal, M. M. (2008). *Intelligence: From secrets to policy* (4th ed.). Washington, DC: CQ Press.

Mathiason, N., Parsons, V., & Jeory, T. (2015). *Europe's refugee crisis: Is Frontex bordering on chaos?*. London: The Bureau of Investigative Journalism. At http://labs.thebureauinvestigates.com/is-frontex-bordering-on-chaos/. Accessed 19 Sept 2015.

McAuley, C. D. (2005). *Strategic implications of imagery intelligence*. Carlisle Barracks: U.S. Army War College.

Mercado, S. C. (2005). Reexamining the distinction between open information and secrets. *Studies in Intelligence, 49*(2). At http://www.cia.gov/csi/studies/Vol49no2/reexamining_the_distinction_3.htm. Accessed 29 June 2008.

Müller-Wille, B. (2002). EU intelligence co-operation. A critical analysis. *Contemporary Security Policy, 23*(2), 61–86.

Müller-Wille, B. (2008). The effect of international terrorism on EU intelligence cooperation. *Journal of Common Market Studies, 46*(1), 49–73.

Nomikos, J. (2014). European Union Intelligence Analysis Centre (INTCEN): Next stop to an agency? *Journal of Mediterranean and Balkan Intelligence, 4*(2), 5–13.

Olcott, A. (2014). *Open source intelligence in a networked world*. London/New York: Continuum.

Omand, D. (2000). *Securing the state*. London: Hurst.

Omand, D., Bartlett, J., & Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security, 27*(6), 801–823.

Omand, D., Miller, C., & Bartlett, J. (2014). Towards the discipline of social media intelligence. In Ch. Hobbs, M. Moran, & D. Salisbury (Eds.), *Open source intelligence in the twenty-first century. New approaches and opportunities*. Basingstoke/New York: Palgrave Macmillan.

Patton, K. (2010). *Sociocultural intelligence: A new discipline in intelligence studies*. London/New York: Continuum.

Phythian, M. (2013b). Introduction. Beyond the intelligence cycle? In M. Phythian (Ed.), *Understanding the intelligence cycle*. London/New York: Routledge.

Politi, A. (2003). The citizen as 'intelligence minuteman'. *International Journal of Intelligence and CounterIntelligence, 16*(1), 34–38.

RAND (2012). *Feasibility study for a European cybercrime centre*. At http://www.rand.org/content/dam/rand/pubs/technical_reports/2012/RAND_TR1218.pdf. Accessed 14 Sept 2013.

Rettman, A. (2011, April 12). EU intelligence bureau sent officers to Libya. *EU Observer*. At http://euobserver.com/9/32161?print=1. Accessed 14 Apr 2011.

Richelson, J. T. (1997). From Monarch Eagle to Modern Age: The consolidation of U.S. defense HUMINT. *International Journal of Intelligence and CounterIntelligence, 10*(2), 131–164.

Richelson, J. T. (1999). *The U.S. intelligence community* (4th ed.). Boulder/Oxford: Westview Press.

Richelson, J. T. (2012). *The U.S. intelligence community* (6th ed.). Boulder: Westview Press.

Rubin Peled, A., & Dror, H. (2010). HUMINT: Combating corporate crime with a counter-terrorism methodology. *Security Journal, 23*(4), 320–331.

Russell, R. L. (2007b). Achieving all-source fusion in the Intelligence Community. In L. K. Johnson (Ed.), *Handbook of intelligence studies*. London/New York: Routledge.

Shulsky, A. N., & Schmitt, G. J. (2002). *Silent warfare: Understanding the world of intelligence* (3rd ed.). Dulles: Potomac Books.

Sorentino, D. (2011). Socio-cultural intelligence. At http://www.brgresearch-group.com/uploads/Article_-_SocioCultural_Intelligence_-_2011_02_10_02.pdf. Accessed 24 Feb 2012.

Space-Time Insight. (2014). *An introduction to situational intelligence*. San Mateo: Space-Time Insight.

Steele, R. D. (2007). Open source intelligence. In L. K. Johnson (Ed.), *Strategic intelligence* (Vol. 2). Westport/London: Praeger Security International.

Storbeck, J. (1999, March 9). *Open source intelligence: A foundation for Regional Co-operation in Fighting Crime and Establishing a Regional Intelligence Community*. Presentation to the Conference of Eurolntel '99, The Hague. At http://www.oss.net/dynamaster/file_archive/040319/f102cc35cc4fd12a5fe2cc69afce0329/OSS1999-X1-20.pdf. Accessed 12 July 2012.

Svendsen, A. D. M. (2013). Introducing RESINT: A missing and undervalued "INT" in all-source intelligence efforts. *International Journal of Intelligence and CounterIntelligence, 26*(4), 777–794.

Treverton, G. F. (2009). *Intelligence for an age of terror*. Cambridge/New York: Cambridge University Press.

Treverton, G. F., & Gabbard, C. B. (2008). *Assessing the tradecraft of intelligence analysis*. RAND Technical Report TR-293. Santa Monica: RAND Corporation.

Tzanetti, T. (2013). How social media contribute to the transformation of intelligence. *Journal of Mediterranean and Balkan Intelligence, 1*(1), 47–58.

Walsh, J. I. (2006). Intelligence-sharing in the European Union: Institutions are not enough. *Journal of Common Market Studies, 44*(3), 625–643.

WEU (1994, November 9). *The future of the WEU Satellite Centre in Torrejon*. Explanatory Memorandum, Document 1437. At http://www.fas.org/spp/guide/europe/military/weu/index.html. Accessed 7 Jan 2012.

CHAPTER 4

Military Intelligence in the EU

Military intelligence is a specific component of any intelligence community due to its functions, tasks, rules and procedures, as well as its technologies and tools. Its special position not only stems from the organisational logic of national security systems, but is largely the result of the external security environment which determines to a high degree the security and defence policies and strategies of a sovereign nation-state.

Military intelligence refers to military threats, armed violence and military operations engaging state and non-state actors in traditional armed conflicts as well as asymmetric warfare. Traditionally, military intelligence was part of command and control on the operational and tactical levels, aimed at reducing uncertainty on the battlefield and 'dissipating' the Clausewitzian 'fog of war'. It was conceived as a process of 'providing information and analysis to help the commander make more effective decisions in times of conflict' (Rolington 2013, p. 53). As a contribution to the commander's decisions in battle, it should include 'an analysis of the demands military commanders make on intelligence and investigates the various ways in which they can and must compensate for the lack of intelligence' (Handel 1990, p. 3).

Nowadays, military intelligence entails knowledge of a possible or actual enemy and awareness of risks and dangers in the area of operations, enabling rapid reaction and resilience building in case of emerging and protracted threats. Its primary purpose is to support the chain of command involving political institutions and military staff on the strategic

A. Gruszczak, *Intelligence Security in the European Union*,
DOI 10.1057/978-1-137-45512-3_4

level as well as military commanders and units on the operational and tactical levels. It is focused on the strategic assessment of high-risk areas and the balance of armed forces and military capabilities of relevant foreign actors.

Military intelligence in the EU is directly bound up with the Common Security and Defence Policy (CSDP). Therefore, it reflects specific strategic, organisational, functional and political prerequisites which are deeply nested in the ideological construction of EU identity (Kølvraa 2010) and the formation of its 'actorness' in international and global dimensions (Smith 2004b, pp. 180–90; Zwolski 2009; Čmakalová and Rolenc 2012; Gehring et al. 2013). The rationale for these processes was that at the end of the 1990s the leading Member States began to search for alternatives to their national security concepts, which were caught in a post-Cold War 'transitory' setting. The effects of globalisation, 'new wars', the proliferation of threats and the emergence of risks to national security far beyond the scope of states' territorial jurisdiction buttressed an idea of a post-national security paradigm established on the basis of multilateral risk sharing and the pooling of military capabilities (Matlary 2009, p. 7).

The Development of Military Intelligence: From the WEU to an EU Comprehensive Approach

The making of the EU security and defence hub was to a certain extent an exercise in ambitions, visions and expectations of the EU as a global player, a strong actor capable of contributing to global governance and bearing responsibility for concerted actions and operations. In brief, the European Union was to convince the world that it 'has the guts'. The heads of state and government of EU Member States decided to rapidly develop EU military capabilities inasmuch as they deemed it indispensable to tackle emerging security challenges and imminent threats to national security policies. These efforts culminated in the traumatic year 2003 when the EU, despite the 'transatlantic rift' over US-led military invasion of Iraq, managed to launch its first military missions (in Macedonia and the Democratic Republic of Congo), to make arrangements with NATO under the Berlin Plus agreement and to articulate its global outlook in a single document, the European Security Strategy (ESS). The latter heralded the ambitious project of the EU assuming a new global role dealing with threats and helping realise the opportunities of multilateral governance. It was highlighted in the text of the strategy that '[a]ctive policies are needed to counter the new dynamic threats. We need to develop a strategic culture that fosters early, rapid, and when necessary, robust intervention' (The European Council 2003, p. 11).

The formulation of the ESS coincided with the launch of the first European Security and Defence Policy (ESDP) missions and the need to meet all conceptual, logistical and operational requirements, including intelligence, surveillance and reconnaissance capabilities. Military operations carried out by the EU have been clearly limited in their scope, tasks, personnel and equipment. The biggest operation, EUFOR ALTHEA in Bosnia and Herzegovina, initially engaged 7,000 troops (including 6,300 from EU member countries). In 2014, the total number of personnel involved in five military and 11 civilian missions and operations under the CSDP amounted to approximately 6,700 persons, including 5,000 from EU Member States (IMPETUS 2014, pp. 12–15). This was a tiny expeditionary effort, not only in comparison with the UN (almost 100,000 troops and police forces), but also with other regional organisations. Nevertheless, these military and civilian assets needed to be managed in the most efficient manner and effectively protected and secured against material and human losses (Whitman 2006, pp. 111–3; Kirchner 2006).

It is fair to say that tentative proposals, initiatives and activities relating to the building, development and enhancement of intelligence capabilities for the purposes of EU security and defence objectives were already emerging in the early 1990s. The acceleration of EU military and defence cooperation since 1998, largely due to Franco-British compromise on ESDP, aroused embryonic forms of military intelligence developed within the Western European Union as the organisation providing the EU with access to operational capabilities and supporting the Union in the framing of defence aspects of the Common Foreign and Security Policy. However, the declaration adopted at the WEU summit in Petersberg in June 1992 encouraged Member States to launch 'missions' and fulfill 'tasks' contributing to common defence and security through crisis management and military operations. As a result, the Planning Cell was established in 1992 to prepare contingency plans for eventual military operations under WEU auspices and to recommend the necessary command, control and communication arrangements. Earlier, the WEU had taken a decision to set up a Satellite Centre as a cornerstone of a future European space-based system covering intelligence, early warning and defence. The Centre began its activities in 1993 but remained on the non-operational, technical and partly experimental level.

The European Union Military Staff (EUMS), established in 2001, is the core element of the security and defence hub. Its main objective was to provide support and assistance to civilian missions, ensuring that preparation, planning and action coincide with the political agenda and operational requirements. Intelligence support and proper situational awareness were deemed necessary to the effective and comprehensive conduct of civilian missions and crisis-management operations. Appropriate national and multinational intelligence capabilities, intersecting in the EUMS, were decisive for monitoring potential crises, identifying present threats, evaluating risks and anticipating further concerns and challenges.

The wars in the Balkans made the governments of the major WEU members realise that the military contribution of this organisation to peacekeeping and crisis management would be dramatically reduced unless effective operational capabilities were built and effectively set in motion. In May 1995, during the final phase of the war in Bosnia, foreign affairs and defence ministers gathering in Lisbon agreed to establish a Situation Centre and an Intelligence Section in the Planning Cell (WEU 1995b). This was subsequently underlined in an important strategic document, 'European Security: a Common Concept of the 27 WEU Countries', adopted by foreign ministers of the WEU nations in November 1995 in Madrid, which stated that the WEU needs 'to establish or to have access to an adequate observation capability and to develop an intelligence processing capability which are decisive for the conduct of operations in complex, shifting politico-military environments' (WEU 1995a, pp. 6–10).

The Intelligence Section and the Situation Centre constituted the germ of the WEU intelligence community, working side by side although using different methods and operating with distinct categories of information and intelligence. As Oberson noted, intelligence support offered by the Intelligence Section was of 'a politico-strategic type rather than tactical' (Oberson 1998, p. 21), meaning that in any given mission the responsibility for a proper intelligence assessment lay with the lead nation supposedly having the best knowledge and orientation in the area of operations. Unlike the Intelligence Section, which was supplied by Member States with mostly classified sources, the Situation Centre operated on the basis of open sources. It aimed to prepare situation reports and disseminate them at the request of the Council to the states attending the meetings of the Permanent Council. The WEU Satellite Centre was also upgraded in 1995 to a permanent subsidiary body and in the following years launched a direct image-receiving system enabling the processing and analysis of imagery delivered by government and commercial satellite providers.

The real contribution of these intelligence units to the operational capabilities of the WEU was fairly limited and did not dispel doubts concerning certain requirements of fledgling European defence cooperation. Meanwhile, the late 1990s brought a series of political declarations and decisions concerning the establishment of permanent political and military bodies in the framework of the common European policy on security and defence. This led to the conclusions adopted by heads of state and government in Helsinki in December 1999 on developing the EU's military capabilities. It was agreed there that a new permanent political and military structure should be established at EU level, including among others a military staff positioned within the Council structures. This shift in the centre of gravity from the WEU to the EU Common Security and Defence Policy had certain, often far-reaching consequences for political, organisational and decision-making arrangements and procedures (Trybus 2005, pp. 97–100; Bickerton et al. 2011, pp. 4–5; Thym 2011, pp. 453–6). The Capabilities Commitments and Capabilities Improvement Conferences held at the end of 2000 and 2001 by EU defence ministers revealed permanent shortcomings, among other things in early warning and military intelligence units, as well as imagery and signal intelligence collection (House of Lords 2002).

The Military Staff, inaugurated in 2001, was tasked with the provision of 'military expertise and support to the CESDP [Common European Security and Defence Policy], including the conduct of EU-led military crisis management operations. The Military Staff will perform early warning, situation assessment and strategic planning for Petersberg tasks including identification of European national and multinational forces' (European Council 1999, p. 89). The Satellite Centre and the Situation Centre (former WEU units) were incorporated into the EU legal-institutional framework and began operating in a relatively new strategic environment.

The building of a military intelligence hub in the new institutional context was a hard and demanding task. The rapid deterioration of the European and global security environment in the aftermath of 9/11, followed by NATO's intervention in Afghanistan, the US-led invasion of Iraq and subsequent tragic episodes in the 'war on terror' occurring in EU countries (Spain and the UK), produced a paradoxical reaction from EU Member States. While they were eager to adopt EU legal measures and organisational arrangements for strengthening the prevention of and fight against terrorism, as well as enhancing practical cooperation in the area of counter-terrorism, in reality they preferred national solutions and activities, relying on pre-established bilateral collaboration patterns including, first and foremost, intelligence sharing. The understanding of terror networks and insurgent groups and the identification of new threats to national security entailed the granting of improved access to secret and sensitive data possessed by national intelligence services and shared with selected partners on a highly secured basis (Svendsen 2010, Chap. 3; Chin 2012, pp. 27–43; Utley 2012, pp. 45–64). The dominant position of the United States and the active role of NATO in the post-9/11 security landscape marked by the war on terror and the campaign against 'rogue states', further weakened the prospects for the coordination and reinforcement of EU intelligence cooperation within the nascent military hub.

The first experiences garnered in the civilian and military missions conducted under ESDP led to the conclusion that strategic assessment and operational planning would be considerably improved by the deeper involvement of EU institutions and bodies (Kurowska 2008; Keukeleire 2010, pp. 61–4; Bickerton et al. 2011, p. 6). An informal meeting of defence ministers in Wiesbaden in March 2007 produced a consensus on measures to improve planning and support of operations (Engberg 2014, p. 38). Officials and experts from the Intelligence Division were formally tasked with providing input to advance planning, crisis response, operations and exercises. Their roles included involvement in EUMS planning, participation in mission monitoring teams and provision of intelligence analysis and products (Bagdonas 2010, p. 16). Moreover, the Council agreed measures to improve capabilities in the area of intelligence and information support (Brennan 2009, p. 20).

The Organisational Structure of the EU Military Intelligence Hub

The military intelligence hub in the EU is a functional-structural response to the demands of modern crisis management, military interoperability and the requirement capabilities for Petersberg missions. Despite the fact that the European Union itself has not yet developed autonomous combat capabilities, the CSDP mandates EU institutions and Member States to engage in military operations and authorises them to use military equipment and armaments if needed. This demonstrates that despite critiques of the weaknesses and shortcomings of the EU CSDP (Biscop 2012, 2013; Mattelaer and Coelmont 2013, pp. 33–7), military intelligence has been an indispensable prerequisite for the fundamental objectives of EU security policy, namely containing violent conflicts, managing crises and restoring order and stability in post-conflict environments. During the period in which the Treaty of Lisbon was being negotiated, the military intelligence cooperation network was consolidating around the EUMS Intelligence Division. However, this network was fairly weak, differentiated and in some instances dysfunctional, especially in 'the hot junction' between closed national intelligence services and relatively open EU bodies.

The EU defence and security hub definitely has a looser structure than other intelligence hubs analysed in this book. It is composed of EU agencies and entities largely dependent on Member States' defence intelligence organisations for the availability, quality, usability and delivery of processed information and intelligence. Moreover, secrecy is a factor of great significance for the intelligence workflow. National military intelligence agencies are of strategic importance for information gathering and intelligence sharing. Their contribution, however, depends greatly on standards of information security adopted at EU level protecting the transfer, storage and processing of the information and intelligence released. Due to differences among Member States, these standards in many cases do not meet security thresholds established by national intelligence organisations and are therefore deemed unsatisfactory and unreliable. The organisational structure of EU military intelligence to some extent reflects the problems and dilemmas resulting from the deficit of trust among Member States and appropriate EU institutions and bodies, as well as differing levels of confidence in measures and solutions adopted and practised at the EU level.

The Treaty of Lisbon introduced major reforms of EU foreign and security policy. The EU's principles, strategic objectives and interests in all fields of international relations required a more coherent, better organised and coordinated institutional basis. The multitude of policy fields, objectives and tasks included in the CFSP demanded greater versatility and more effective leadership in the management and implementation of the EU's external affairs (Merlingen and Ostrauskaitė 2008). Functionally, the external dimension of the EU was split between the CFSP, with the CSDP as its integral part, and external economic and humanitarian matters, such as trade, development and humanitarian assistance. Institutionally, the CFSP remained within the remit of the High Representative and Member

States, with the European Parliament and the Commission assuming specific roles. Generally, the position of the High Representative was strengthened, with significant changes in EU security and defence policy corresponding with an expanded role and increased number of tasks for the HR (Thym 2011, pp. 456–8; Denza 2012; Zwolski 2012, pp. 75–6).

In November 2009, at an informal meeting shortly before the entry into force of the Lisbon treaty, EU heads of state and government agreed on the appointment of Catherine Ashton as the High Representative. Adorned with three 'hats' (High Representative for Foreign Affairs and Security Policy / President of the Foreign Affairs Council / Vice-President of the European Commission), she was responsible for putting into effect the Common Foreign and Security Policy.[1]

The European External Action Service (EEAS) was established to synchronise and coordinate external activities at global and regional levels with due reference to the EU's structural framework and decision-making mechanisms. Commencing its operations in 2011, the EEAS was a hybrid combination of institutional segments responsible for diplomacy, external relations and neighbourhood policies, regional development and humanitarian assistance, with additional organisational components responsible for civil and military aspects of security and defence (van Vooren 2011; Duke 2012; Bátora 2013; Juncos and Pomorska 2013, 2014). The HR/VP acted as a coordination hub, linking foreign policy with security and defence. This means that the High Representative, acting in their own capacity or via deputies, and assisted by the Political Affairs Department, is key to the practical and systematic intelligence support for foreign affairs and diplomatic activities within the EEAS's remit. The HR's role in liaising between the CSDP and the common foreign policy was further highlighted by specific arrangements concerning security policy and CSDP structures, especially those concerning the preparation, conduct and management of military missions and tasks (Dijkstra 2012, pp. 457–8).

The Political and Security Committee (PSC) is an auxiliary body assisting the Council in the preparation and management of CSDP missions and operations. Established in 2001, it meets at the ambassadorial level to monitor the international situation and help define policies within the CFSP/CSDP by delivering opinions and providing guidelines on external relations and security matters. The PSC may send guidelines to the Military Committee and receive in return its opinions and recommendations (Longo 2010, p. 75). The PSC prepares a coherent EU response in the event of a crisis, managing the EU's military reaction and exercising political control and strategic direction. It can also contribute significantly to consultations with other security actors, in particular with NATO and the third states involved (Council of the EU 2001a, p. 1). The Treaty of Lisbon did not introduce essential changes to the competences of the PSC (Payne 2010, p. 10). However, it did authorise the HR/VP to appoint his/her representative chairperson of the PSC (Council of the EU 2009a, p. 28). This meant stronger and permanent supervision of the PSC and a direct influence on the organisation and monitoring of PSC activities.

With the establishment of EEAS, better and more effective intelligence support for the decision-making process at the EU level was required. Rather than replicate Member States' existing schemes, methods and resources, specific solutions dedicated to EU institutions and agencies were needed that nonetheless respected sensitive national interests, since those institutions and agencies relied on Member States' intelligence contributions. A new system for managing intelligence workflow between national and supranational levels increased sharing and delivery, while reducing restrictions on access to information and intelligence relating to EU security policy objectives. Not only did this make political sense, but from the point of view of military security it developed and strengthened the intelligence role, making it into a robust institutional mechanism of strategic awareness, preparedness, readiness and resilience, rather than mere support for the armed forces.

The rebuilding of the EU edifice proclaimed in Lisbon and implemented steadily since late 2009 also had important repercussions for military intelligence tradecraft. New organisational structures, identified mainly with the EEAS, new actors and new requirements also meant new challenges and the need for a remodelled, flexible and comprehensive approach to intelligence. The prevailing attitude of both EU officials and representatives of Member States to the challenges and demands of a rapidly changing strategic environment highlighted the need for solid, accurate and active intelligence support for civilian and military operations in terms of threat prevention, early warning, situational assessment and operational reconnaissance.

In the aftermath of the Lisbon reforms, military intelligence cooperation was substantially re-designed, with a refreshed, comprehensive view of EU security producing new strategic and operational requirements.

A European Security Model, outlined in the EU Internal Security Strategy adopted in early 2010, assumed ‘the interdependence between internal and external security in establishing a “global security” approach with third countries’ (General Secretariat of the Council 2010, p. 8) and highlighted the challenge of transnational, common global threats, such as terrorism, violence and radicalisation, organised crime, cybercrime, and natural disasters. Revolutions and rebellions in North and Sub-Saharan Africa, post-conflict stabilisation and reconstruction, the problem of nuclear proliferation, maritime piracy, weak and dysfunctional states—all these hotspots of global security required close observation and surveillance to produce a situational awareness enabling an appropriate reaction to potential risks and emerging crises.

The Intelligence Division (INTDIV) of the EUMS was ‘the focal point for the exchange of military intelligence at the Union level’ (Müller-Wille 2004, p. 23). It was tasked to ‘provide intelligence input to early warning and situation assessment; to contribute to the EUMS planning through the provision of intelligence and intelligence planning expertise; to provide the intelligence input to crisis response planning and assessment for operations and exercises’ (EEAS 2014d). In its early days, the Intelligence Division had hardly any analytical capacities of its own or any intelligence support other than open sources, so the national military intelligence services arranged a voluntary dataflow system that allowed INTDIV to send requests for information via encrypted channels to direct secure access points in national defence organisations. The latter, however, were not bound to provide a response. Their decision depended largely on the category, scale and intensity of quickly emerging threats and the specific intelligence support requirements.

The establishment of the EEAS and the incorporation of the EUMS into the new structures did not change the terms of reference of the Intelligence Directorate (EUMS INT). However, it did bring about a significant change in requirements for intelligence products. The demand for high-quality expertise and intelligence support increased considerably. The volume and variety of intelligence products was also growing. EUMS INT was not only responsible for situational assessments, identifying threats and risks and supporting strategic planning, but also served civilian purposes, providing communication support for risk analysis, estimates of the likelihood of a latent conflict escalating, and lessons learned in comprehensive strategic knowledge management.

EUMS INT is organised into three departments (branches) reflecting the traditional intelligence cycle requirements and division of tasks in military intelligence:

- Intelligence policy;
- Intelligence requirements;
- Intelligence production.

The Policy Branch is responsible, in close cooperation with the relevant civil authorities, for the design and development of intelligence concepts. It also contributes to the planning of EU military operations and prepares intelligence scenarios and specifications for exercises carried out under the CSDP. It has also been responsible, since 2001, for organising an annual conclave of heads of military intelligence organisations from EU Member States, held as a one-day closed session (European Parliament 2011). The conclave is an informal forum for the exchange of views and opinions as well as the improvement of coordination mechanisms between national defence intelligence services and the EUMS. It often develops into a constructive discussion about ways of supporting intelligence cooperation at EU level, mainly through strong and substantial contributions from Member States to the analytical and intelligence capabilities of relevant EU agencies and bodies (European Parliament 2012a). The European Union is represented by the Intelligence Director at EUMS.

The Requirements Branch is responsible for strengthening cooperation with the military intelligence agencies of Member States. It manages the flow of information and intelligence between the Intelligence Directorate and the national defence intelligence services. It facilitates regular meetings of members of intelligence agencies from EU Member States. A system of national points of contact ensures constant and direct links between EUMS INT and military intelligence agencies (Vaz Antunes 2005, p. 68). The Requirements Branch also makes a valuable contribution to the development of ISTAR capability, co-ordinating inputs from national representatives and integrating them with materials handed over by relevant EU institutions and bodies and other appropriate stakeholders. This branch cooperates with the EU Satellite Centre in the area of geospatial intelligence support for situation assessment, strategic reconnaissance and crisis response planning.

The Production Branch is the central element of the Intelligence Directorate. Its function is to ensure that intelligence production meets the needs of EU institutions and bodies. Analysts working in this department are grouped into five thematic and regional task forces and one task force for transnational issues. The department works closely with the EU Intelligence Analysis Centre (INTCEN) using the SIAC mechanism (for more on SIAC see Chap. 9), and prepares joint, multi-source intelligence products (Haag and Anaya 2011, p. 8). Apart from contributing to all-source situation assessments, the Production Branch also prepares intelligence briefs on a regular basis and delivers 'on-the-spot' intelligence assessments for the Military Staff, the Military Committee, and the HR/VP (Vaz Antunes 2005, p. 68). It also cooperates with the EU Satellite Centre through a separate cell for geospatial support. This cell provides expert assistance to other bodies of the Military Staff, Board of Planning and Crisis Management and the appropriate EEAS authorities on the practical use of products supplied by the Satellite Centre.

The Sources of Military Intelligence

The analytical capabilities of the EU security and defence sector have been, from the beginning, largely dependent on Member States. Although the value and importance of open-source information has gradually increased, the defence intelligence organisations of EU Member States have been central to the actual input and workflow of information and intelligence within the EU defence and security hub. The EUMS INT is the central analytical node in this structure. It is fed by other EU units, namely SATCEN and INTCEN, which provide geospatial intelligence and analytical products from the inputs of national civilian intelligence services.

The EUMS Intelligence Directorate, like its predecessor, the Intelligence Division, has had to rely principally on classified contributions from the military intelligence services of Member States, processed and shared by national intelligence services and delivered to EUMS via national points of contact. Günter Eisl, former Intelligence Director at EUMS, said: 'We don't get raw material. We get finished intelligence already analysed by member states. Our role is to put all together' (Guarascio 2011). In a similar vein, Eisl's predecessor Gintaras Bagdonas pointed out that 'EUMS intelligence is bound to the Member States Defence Intelligence Organizations (DIO), which are the main providers of intelligence inputs' (Bagdonas 2008, p. 8). He added that all procedural and organisational issues concerning military intelligence workflow needed to be consulted with national military intelligence services.

The preparation and planning of military missions require precise imagery of geographical and geophysical environments. Visual observation and surveillance, as well as geospatial analysis of physical features and geographically referenced activities in the area of military operations, have been widely implemented due to technological advances and multi-level and all-source analysis tools, as well as easier and wider access to geospatial data (Darnis and Veclani 2011, pp. 5–9). It is worth remembering that decisions to enhance the capacity to use satellite imagery for security purposes were among the initial elements of the European security and defence identity and policy which began to be built by the Western European Union in the mid-1990s (WEU 1995b, p. 30). Since the establishment of the EU Satellite Centre, geospatial intelligence capabilities have been gradually yet systematically developed as a result of the deepening cooperation between SATCEN and Member States. By 2015, the EU Satellite Centre was capable of obtaining satellite imagery and collateral data from state-owned and commercial satellites. Civilian satellite images are purchased on a case-by-case basis, the main provider being the US company DigitalGlobe (Quickbird, Ikonos, Worldview, GeoEye satellites). Other companies from Canada, Israel, India, Taiwan and South Korea are also occasional SATCEN suppliers.

As to EU Member States, SATCEN's focus is on government satellite systems. Economic, technological and security reasons lie behind the increased interest in the development of state-owned satellite sensors. First, images and geospatial data obtained from governments are free of charge, which is particularly important in view of the decrease in SATCEN's budget. The quality and resolution of satellite imagery and the accuracy of data from synthetic aperture radars match products offered by private companies. However, these companies rarely use the maximum technical capabilities of satellite sensors, and they demand high fees for pictures of the highest quality. Second, commercial providers use different technologies to offer a variety of geospatial services, including imagery of a delimited surface, multispectral imagery, geo-visualisation and geospatial data collection including geological, geographical, spatial, hydrological, meteorological and ecological datasets. Geospatial analysis performed at SATCEN often requires access to various types of geodata held by different commercial providers. Those data cannot be delivered quickly and sometimes their purchase is subject to negotiation. As a result, SATCEN is forced into the fairly lengthy and tedious collection of geospatial products from dispersed sources.[2] Third, images and geospatial data from private companies are uploaded to SATCEN using low-level security safeguards and open internet connections. Security systems for government sensors are much more advanced and allow for the transfer of classified geospatial information.

These arguments highlight the structural and organisational barriers to the acquisition, transfer and processing of geospatial data faced by SATCEN in delivering geospatial intelligence products to relevant customers in the EU and Member States, whose engagement in the improvement process is determined by their technical, technological and financial capabilities. France, the most active stakeholder, heads a consortium with Italy and Spain which constructed the Helios military optical reconnaissance system, in operation since the mid-1990s. In 2001, the consortium was enlarged to include Germany, Belgium and Greece and stepped up to the next-generation Helios system (Helios II). France is also a party to two other agreements on satellite cooperation. The first, Helios SAR-Lupe, is a joint French-German space-based reconnaissance network project that integrates the French Helios II system with the German synthetic aperture radar (SAR) system SAR-Lupe. SAR data is the only satellite imagery that can be acquired at any time, during adverse weather conditions and in remote or hardly accessible areas. Another joint project launched in 2001 by France and Italy focused on Optical and Radar Federated Earth Observation (ORFEO). It provided for the construction of a multi-sensor satellite data collection system connecting very high-resolution optical sensors installed on two French Pléiades satellites and SAR equipment located on four satellites of the Italian COSMO-SkyMed system. The latter is an Italian dual-use system for both commercial and government satellite imagery (Berger et al. 2012, pp. 84–90).

In the early 2000s some defence ministries of Member States complained that satellite output was slow and of poor quality, limiting the usefulness of the EU Satellite Centre (Pasco 2004, p. 24). Since then, however, progress in national GEOINT capability development, as well as in geospatial data analysis and geospatial intelligence production by SATCEN, has been indisputable. First of all, the agency gained continuous access to government satellite imagery and geodata using secured communication networks. In 2008 SATCEN concluded an agreement on permanent access to optical imagery from Helios II (EUSC 2010, p. 15). The agency established a secure direct electronic communication link with the ground segment of SAR-Lupe. The connection was declared fully operational in 2013 and has been used to download SAR-Lupe classified imagery (EUSC 2014b, p. 20). In 2008, the EU signed an agreement on access to COSMO-SkyMed government imagery (EUSC 2010, p. 15). The EU Satellite Centre has also been a partner in research projects related to geospatial intelligence. It was involved in the Copernicus/GMES project, implemented by the European Space Agency, which combines satellite imagery and data with local data sources to deliver geospatial information services and products to a wide range of customers (Aschbacher and Milagro-Pérez 2012, pp. 3–8; BRIDGES 2013, pp. 2–3). The first component of the system, Sentinel-1 satellite, was put into Earth orbit in April 2014. Further efforts were made to increase access to high-resolution imagery, mostly from government satellites, a timely and precise source of information essential for effective preparation and support for CSDP missions and operations (EDA 2013, pp. 17–18). In 2013, very high-resolution images constituted 95 per cent of all sensor data downloaded by SATCEN (EUSC 2013, p. 22). Since the late 2000s SATCEN has developed intensive cooperation with the European Defence Agency (EDA), participating in several projects to enhance military ISR capabilities (intelligence, surveillance, reconnaissance) and OSINT (EUSC 2011, p. 25).

SATCEN's increasing involvement in support of EU operations and missions reflects the changing international environment and the emergence of new poles of tension and conflict such as North Africa during and after the Arab Spring, or maritime piracy in the Western Indian Ocean. Enduring threats and risks in traditional crisis areas such as the Middle East, the Balkans, Sub-Saharan Africa or the Caucasus affect the foreign and security policies of the EU. The EEAS's decision-making process has become more complex and dependent on good situational assessment and risk analysis, especially when the use of substantial security policy instruments and methods, including military force, has been under consideration by Member States. SATCEN's position in the military hub has been strengthened, mainly as a result of pressure on EEAS from Member States which were vitally interested in improving the operational capabilities of EU forces and minimising the probability of human, financial and material losses as well as political and strategic failures.

The EU Intelligence Analysis Centre is another specific source of intelligence that has gradually evolved from 'a sort of empty shell',[3] disconnected from dynamic changes in the European security landscape, into a well organised analytical unit delivering numerous strategic intelligence products built on all-source analysis. INTCEN was originally set up under the WEU in 2002 as the EU's Joint Situation Centre, attached to the Office of the High Representative for CFSP. It was created in response to several Member States voicing the need to encourage national governments to improve information exchange and streamline intelligence flows. As a unit active in the field of European security and defence policy, SITCEN focused on threats posed to the Union by the proliferation of weapons of mass destruction, the trafficking of arms and other global issues (House of Lords 2003, p. 25; European Parliament 2009; Nomikos 2014, pp. 10–11). A separate task concerned terrorist threats and the EU strategy for preventing and combating terrorism (Bigo et al. 2007, p. 41). In the aftermath of 9/11, SITCEN was contributing to CFSP anti-terrorist measures such as terror blacklists, and providing available input drawn mostly from open sources and partially from intelligence delivered by national civilian intelligence agencies.

SITCEN was a kind of facilitator for the intelligence services of major EU Member States to exchange processed security-related information (Davis Cross 2013c, p. 393). It worked on open-source material, and military and non-military intelligence from several Member States, as well as diplomatic reporting. It was focused on matters related to the ESDP, crisis-management missions, forthcoming military and civilian operations, and immediate reactions to new threats which needed to be tackled by a mixture of military and civilian instruments. Hence, from the early days of SITCEN's activities a number of military officers from the EUMS Intelligence Division were incorporated within the Centre (Müller-Wille 2008, p. 62), signalling a growing tendency to strengthen ties between military and civilian intelligence and, by adding open-source analysis to it, to work out a specific multi-source approach to the most critical aspects of EU security policies. For operational reasons, the High Representative Javier Solana put forward a proposal for 'bring[ing] together, in a functional way, the analytical capacities from both the EU Situation Centre (SITCEN) and EUMS INT, thus benefiting from a wider knowledge base for producing enhanced and more reliable Intelligence' (Haag and Anaya 2011, p. 8).

During the 2006 Lebanon war Javier Solana sought to strengthen the EU's role in the Middle East, offering mediation and assistance to de-escalate the conflict. He quickly realised how important a good situation assessment is and asked SITCEN and EUMS INT for a joint endeavour that could build situational awareness and enhance risk-assessment capacity (Engberg 2014, pp. 66–7). As a result, the Single Intelligence

Analysis Capacity (SIAC) was established in 2007 with the aim of pooling civilian intelligence obtained by the then SITCEN with early warning and situation-assessment input provided by EUMS INT (see Chap. 9).

The defence and security hub increasingly exploits open sources of information and intelligence made available by respective national authorities. OSINT is also drawn from EU sources: information, reports and dispatches coming from EU diplomatic representatives, officials participating in EU-led missions and operations, EU agencies and units (SATCEN, INTCEN, EDA) in the case of deliverables based exclusively on open sources. Moreover, mass media, especially electronic and social media, are monitored in the context of CSDP-related strategic goals and operational tasks. Finally, commercial databases and strategic intelligence services purchased from independent analysis and advisory companies like The Economist Group (Economist Intelligence Unit), Oxford Analytica, LexisNexis and IHS Inc. (Jane's) are also exploited.

Military Intelligence Tradecraft

EUMS INT does not simply compile national inputs and OSINT analyses in situ. It receives information and data provided by Member States' military intelligence services. According to an arrangement worked out in the early stages of the establishment of EUMS, the Intelligence Directorate may send a request for information to national defence intelligence services through a secure encrypted messaging service. This system links national intelligence organisations with EUMS INT, ensuring quick communication in the face of urgent information needs, suddenly emerging threats or intelligence support requirements (Haag and Anaya 2011, p. 8). Member States should provide a rapid response, albeit on a voluntary basis. In the case of positive reaction to a threat or a security breach, a national intelligence organisation should deliver a secured set of prepared information and intelligence in response to the needs of the originator. The 'ownership' of intelligence is a factor regulating further circulation of a given file. The delivering state may limit access to the file according to the need-to-know principle or the specific reason for supplying it. Any use of the file for additional analysis needs the formal consent of the delivering state. As a result, the receiving states or EU agencies and bodies cannot be certain that they will receive all the relevant intelligence in a single package. Nor can they rule out the possibility that original 'raw' data may be modified or distorted.

Even if the national provider authorises the Intelligence Directorate to make use of intelligence data it has shared for further analytical activities, the source of this data is covert. Therefore, the users cannot identify the originator of the file unless they want to process it further. In that case, they must approach the country that provided the original information and request the appropriate permission. This rule has a dual purpose. First, it provides a safeguard that the information supplied by a national source to an EU agency or unit will be used exclusively for the stated purpose. Moreover, it prevents EU bodies from passing on this information or using it for purposes unrelated to the original aim. Second, it encourages Member States to share the information and finished intelligence they hold with other partners and to supply strategic intelligence to the Intelligence Directorate (Walsh 2009, p. 15).

The protection of classified information provided by national military intelligence agencies and processed by EUMS INT, and sometimes shared with other EEAS intelligence agencies and bodies, is a highly sensitive and demanding issue. It requires EU institutions to establish and maintain a secure communication network to protect sensitive and classified data which, if compromised, would jeopardise the national interests of intelligence providers as well as the ability of EU bodies to achieve their strategic and operational objectives (Robinson and Gaspers 2014, p. 56). Classified information for strategic intelligence analysis relating to CSDP is exchanged between Member States and EUMS through the encrypted information system ESDP-Net. This network was established in the mid-1990s and has been constantly updated. It enables fast and secure classified information exchange to improve and strengthen situational awareness building, decision making and planning in the area of CSDP (DGA 2011, p. 32). Any transmission of classified information within ESDP-Net is subject to the adoption of protection tools, communication channels and operating procedures specifically approved by the Security Accreditation Authority for this purpose (Council of the EU 2006a).

Following the adoption in 1999 of the Helsinki headline goals, defence ministers from Member States decided to build a new secure communication network to support classified information exchange in the CFSP and ESDP domain (DGA 2011, p. 32). The SESAME network has been under development by the Council since 2002. The initial target implementation date has been postponed several times due to technical obstacles and disagreement among Member States over ways and means of protecting sensitive information, as well as the rigorous accreditation procedure for obtaining the Council's security clearance (Court of Auditors 2009, p. 217). By the end of 2014 SESAME was still inactive, contrary to some announcements from the Commission on the 'rolling out' of the system.[4]

Certain categories of information and intelligence are exchanged via the EU Operations Wide Area Network (EU OPS WAN). It connects EU bodies, Member States and military operational headquarters established within the EU in the context of the planning and command of military operations under CSDP (Council of the EU 2009a). The EU OPS WAN also serves geospatial intelligence and data transmission from the EU Satellite Centre to relevant Member States. The network has been progressively expanded to connect more national points of contact to SATCEN (EUSC 2013).

The overall production of military intelligence responds to the fundamental objectives of the defence and security hub, namely the delivery of intelligence input for strategic planning, situational assessment and emergency response. Its products are submitted to relevant national authorities of Member States, including their military intelligence organisations. They are also made available to respective security and defence bodies in the Council of the EU to the extent permitted by those Member States that deliver a given input to the processing and analysis of intelligence material. The European Parliament may also be the recipient of classified intelligence under the terms of the interinstitutional agreement between the European Parliament and the EEAS (Council of the EU 2009b).

The Impact of Military Intelligence on the EU Security and Defence Policy

The establishment and development of the EU military intelligence hub has been determined by the predominance of vertical cooperation led by Member States and driven by their own national security strategies. Common defence and security building through military means and support for operations 'out of EU area' has been hindered by the deficit of political will on the part of Member States and the political ambitions of a Commission and HR/VP seeking global security player status for the EU. However, political endorsement of the concept of military operations and its subsequent development in the framework of the European Security and Defence Policy has led to the creation and progressive expansion of appropriate institutional arrangements at EU level. The establishment of the EUMS Intelligence Division and the formation of the Joint Situation Centre and the Satellite Centre have expanded intelligence capabilities, supporting both EU strategic objectives and national interests.

The development of intelligence cooperation within the EU's security and defence hub has been a test case for Member States' credibility and willingness to deliver their intelligence assets to a common pool of strategic resources regardless of information security concerns and communication barriers. The first decade of the twenty-first century witnessed civilian missions and military operations which were almost entirely dependent on national intelligence support subject to political consent, restrictive safeguarding measures and case-by-case decision making. Supplementary intelligence, drawn mostly from open sources, could fill some strategic and operational gaps but it could not address critical problems that emerged during the ongoing missions and operations. Against this background, the nascent EU intelligence entities operated in clear separation from each other and it was only in the mid-2000s that they began establishing channels for delivering and sharing available intelligence materials. This practice was nonetheless confined to open-source intelligence and such intelligence products as were released by national intelligence services for further circulation. Attempts to merge information and intelligence originating in EU bodies, such as the SIAC arrangement, were partially successful. Nonetheless, even positive outcomes of the EU civilian-military intelligence collaboration scheme could not compensate for the systemic obstacles undermining progress in all-source analysis and a comprehensive approach to military intelligence.

The reconfiguration of the EU security and defence intelligence hub following the 2009 treaty reform raised expectations of a reinforcement of intelligence tradecraft, analytical capabilities and information sharing within the new institutional framework provided by the EEAS. It was at this time that two EUMS officers proposed a transformation of EU military intelligence cooperation from the 'need-to-know' principle towards a 'responsibility to share' (Haag and Anaya 2011, p. 9). However, there is always a degree of sensitivity about sharing intelligence material originating in national organisations.[5] The major state actors preferred solutions which had been in force since the beginning of military intelligence cooperation and were not ready to acknowledge that the planning, launching and carrying out of EU missions and operations engages national capabilities and resources which could be better protected if EU intelligence bodies were regarded as reliable partners and honest brokers in the preparation and coordination of CSDP actions.

The quality of strategic intelligence partly depends on operational and tactical assets that are generally in the hands of Member States. However, tasking Member States whose forces are dispatched on a CSDP mission with collecting, processing and delivering information to EU intelligence units has been problematic.[6] This has to do with the content, scope and aim of the mission, which determine the composition of EU contingents. Former US Defence Secretary Donald Rumsfeld's argument that the 'mission defines the coalition' seems to be valid also with regard to EU Member States. Lieutenant General Ton van Osch, Director General of the EU Military Staff in 2010–2013, noted that 'Member States would rather contribute to a mission with a high possibility of success, than become part of an operation with high risks' (van Osch 2013, p. 4). Many military operations in the preparation and planning phase focus on situational awareness, risk assessment, environment scanning and other methods of securing and protecting the human and material assets expected to be deployed. The first reaction to the rising tide of piracy off the coast of Somalia was the setting up of the Mission Monitoring Team (MMT) within EUMS which aimed, in the words of the first leader of the team, Lt. Col. Tim Cook (2010, p. 6), 'to provide impartial advice at the strategic level to an operation specifically on the management and staffing of issues through Brussels'. With the launch of EUNAVFOR Somalia—Operation ATALANTA—at the beginning of December 2008, the MMT was tasked by EUMS with specific issues concerning the dynamic of the strategic environment, ensuring situational awareness and delivering information and estimates to the office of the Chairman of the EU Military Committee. An increasing involvement of EU agencies and units in strategic assessment and operational planning was evidenced in the case of the geospatial support offered by SATCEN for CSDP missions in North Africa and the Sub-Saharan region, and INTCEN's situation and risk assessments and special reports.

Military intelligence cooperation plays an auxiliary role in the EU's CSDP. The agencies and units involved in intelligence support for EU-led military operations have played a small part in the development of security and defence policy, highlighting situational awareness, risk assessment and strategic intelligence elements. For political reasons, they remain dependent on Member States' intelligence input. Nevertheless, they strive to link the sparse secret and classified information delivered by national intelligence services with OSINT and EU-owned information. This is a relatively limited contribution but it cannot be neglected by sovereign decision makers in Member States.

Notes

1. See Article 24.1. of the Treaty on the European Union (European Union 2012, p. 30).
2. Anonymous SATCEN official, interview, June 2012.
3. The statement of William Shapcott, Director of the Joint Situation Centre and Special Adviser to Javier Solana, in: House of Lords 2005, p. 54.
4. Anonymous EEAS official, interview June 2015.
5. Anonymous EEAS official, interview June 2012; anonymous European Commission official, interview June 2012.
6. Anonymous national military official from an EU Member State, interview January 2014.

Bibliography

Aschbacher, J., & Milagro-Pérez, M. P. (2012). The European earth monitoring (GMES) programme: Status and perspectives. *Remote Sensing of Environment, 120*, 3–8.

Bagdonas, G. (2008). Sharing capabilities. *Impetus. Bulletin of the EU Military Staff, 6*, 8–9.

Bagdonas, G. (2010). Evolution of EUMS intelligence directorate and a way ahead. *Impetus. Bulletin of the EU Military Staff, 9*, 16.

Bátora, J. (2013). The 'mitrailleuse effect': The EEAS as an interstitial organization and the dynamics of innovation in diplomacy. *Journal of Common Market Studies, 51*(4), 598–613.

Berger, M., et al. (2012). ESA's sentinel missions in support of Earth system science. *Remote Sensing of Environment, 120*, 84–90.

Bickerton, C. J., Irondelle, B., & Menon, A. (2011). Security co-operation beyond the nation-state: The EU's common security and defence policy. *Journal of Common Market Studies, 49*(1), 1–21.

Bigo, D., et al. (2007). Mapping the field of the EU internal security agencies. In D. Bigo (Ed.), *The field of EU internal security agencies.* Paris: L'Harmattan/Centre d'Etudes sur les Conflits.

Biscop, S. (2012). The UK and European defence: Leading or leaving? *International Affairs, 88*(6), 1297–1313.

Biscop, S. (2013). Peace without money, war without Americans: Challenges for European strategy. *International Affairs, 89*(5), 1125–1142.

Brennan, Ph. (2009). Post-Wiesbaden 'new' considerations on intelligence development. *Impetus. Bulletin of the EU Military Staff, 8*, 20–21.

BRIDGES (2013). Copernicus demystified. *Window on Copernicus*, Special Issue. At http://www.gmes-bridges.eu/sites/gmes-bridges.eu/files/Window%20on%20GMES%20-%20G-MOSAIC%20-%20Special%20Issue%20on%20Security.pdf. Accessed 22 Aug 2014.

Chin, W. (2012). Ten years of Britain's war against Al Qaeda. In R. E. Utley (Ed.), *9/11 ten years after: Perspectives and problems.* Farnham/Burlington: Ashgate.

Čmakalová, K., & Rolenc, J. M. (2012). Actorness and legitimacy of the European Union. *Cooperation and Conflict, 47*(2), 260–270.

Cook, T. (2010). OP ATALANTA—The role of the MMT. *Impetus. Bulletin of the EU Military Staff, 9*, 6–7.

Council of the EU (2001a, January 30). Council decision of 22 January 2001 setting up the Political and Security Committee (2001/78/CFSP). *Official Journal of the European Communities, L 27*, 30.

Council of the EU (2006a). Guide on the security of information: September 2006. At http://bookshop.europa.eu/en/guide-on-the-security-of-information.-september-2006-pbQCX106131/downloads/QC-X1-06-131-EN-C/QCX106131ENC_001.pdf. Accessed 12 Oct 2013.

Council of the EU (2009b, November 17). Council conclusions on military capabilities (extract from council conclusions on ESDP) 2974th External Relations Council meeting Brussels. At http://www.consilium.europa.eu/uedocs/cmsUpload/Military_capabilities_EN.pdf. Accessed 19 Nov 2009.

Council of the EU (2009c, May 15). Council decision of 6 April 2009 establishing the European Police Office (Europol). *Official Journal of the European Union, L 121*.

Court of Auditors (2009, November 10). 2008 Annual report on the implementation of the budget. *Official Journal of the European Union, C 269*.

Darnis, J.-P., & Veclani, A. C. (2011). *Space and security: The use of space in the context of the CSDP*. Strasbourg: European Parliament.

Davis Cross, M. K. (2013c). A European transgovernmental intelligence network and the role of IntCen. *Perspectives on European Politics and Society, 14*(3), 388–402.

Denza, E. (2012). The role of the High Representative of the Union for Foreign Affairs and Security Policy. In H.-J. Blanke & S. Mangiameli (Eds.), *The European Union after Lisbon. Constitutional basis, economic order and external action*. Berlin/Heidelberg: Springer-Verlag.

DGA (2011). *DGA communication and information systems. 2010 Activity Report.* At http://bookshop.europa.eu/pl/dga-communication-and-information-systems-pbQCAL11001/;pgid=Iq1Ekni0.1lSR0OOK4MycO9B0000y58nN1Sb;sid=rv3kHr3MvnfkE-v1jLF6ud_pDD6YTh8P0q0=?CatalogCategoryID=luYKABst3IwAAAEjxJEY4e5L. Accessed 11 Jan 2012.

Dijkstra, H. (2012). Agenda-setting in the common security and defence policy: An institutionalist perspective. *Cooperation and Conflict, 47*(4), 454–472.

Duke, S. (2012). The European external action service: Antidote against incoherence? *European Foreign Affairs Review, 17*(1), 45–68.

EDA (2013, October 15). Final report by the High Representative/Head of the EDA on the Common Security and Defence Policy, Brussels, pp. 17–18.

EEAS (2014d). EUMS organisations. At http://eeas.europa.eu/csdp/structures-instruments-agencies/eu-military-staff/organization/index_en.htm. Accessed 14 Mar 2015.

Engberg, K. (2014). *The EU and military operations: A comparative analysis.* London/New York: Routledge.

European Council (1999). European Council. Helsinki, 10–11 December 1999. In *From St-Malo to Nice. European defence: core documents.* Chaillot Paper no. 47. Paris: EU Institute for Security Studies.

European Council (2003, December 12). *A secure Europe in a better world. European Security Strategy.* Brussels.

European Parliament (2009, December 1) Answer to the written question E-5998/09 from Martin Ehrenhauser, MEP, to the Council. Subject: Policy Planning and Early Warning Unit. At http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2009-5998&language=EN. Accessed 8 Mar 2013.

European Parliament (2011, August 12). Answer given by High Representative/Vice-President Ashton on behalf of the Commission to the written question E-6392/2011 put by Martin Ehrenhauser (NI) to the Commission. Subject: VP/HR—Intelligence Division (INT). At http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2011-006392&language=EN. Accessed 8 Mar 2013.

European Parliament (2012a, August 24). Answer given by High Representative/Vice-President Ashton on behalf of the Commission to the question E-006024/2012 from Martin Ehrenhauser, MEP. Military Staff Intelligence Directors Conclave and 'Community of Interest'. At http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2012-006024&language=EN. Accessed 8 Mar 2013.

European Union (2012). Treaty on European Union (consolidated version). *Official Journal of the European Union*, C 326, 26 October.

EUSC. (2010). *EUSC annual report 2009.* Luxembourg: Publications Office of the European Union.

EUSC. (2011). *EU Satellite Centre annual report 2010.* Luxembourg: Publications Office of the European Union.

EUSC. (2013). *EU SatCen annual report 2012.* Luxembourg: Publications Office of the European Union.

EUSC. (2014b). *EU SatCen Annual Report 2013.* Madrid: EU SatCen.

Gehring, Th., Oberthür, S., & Mühleck, M. (2013). European Union actorness in international institutions: Why the EU is recognized as an actor in some international institutions, but not in others. *Journal of Common Market Studies, 51*(5), 849–865.

General Secretariat of the Council. (2010). *Internal security strategy for the European Union. Towards a European security model.* Brussels: General Secretariat of the Council.

Guarascio, F. (2011). No plans for EU secret intelligence operations. *Public Service Europe*, 23 September. At www.publicserviceeurope.com/article/898/no-plans-for-eu-secretintelligence-operations. Accessed 7 Mar 2013.

Haag, D., & Anaya, C. B. (2011). The first ten years of military Intelligence Support for the work of the EU. *Impetus. Bulletin of the EU Military Staff, 11*, 8–9.

Handel, M. I. (1990). Intelligence and military operations. In M. I. Handel (Ed.), *Intelligence and military operations.* Abingdon: Routledge.

House of Lords (2002). *The European Policy on security and defence*, vol. 1. HL Paper 71 (I). London: The Stationery Office.

House of Lords (2003). *EU – Effective in a Crisis?* HL Paper 53. London: The Stationery Office.

IMPETUS (2014). EU Missions and operations. *Impetus. Magazine of the EU Military Staff, 18*, 12–15.

Juncos, A. E., & Pomorska, K. (2013). 'In the face of adversity': Explaining the attitudes of EEAS officials vis-à-vis the new service. *Journal of European Public Policy, 20*(9), 1332–1349.

Juncos, A. E., & Pomorska, K. (2014). Manufacturing Esprit de Corps: The case of the European external action service. *Journal of Common Market Studies, 52*(2), 302–319.

Keukeleire, S. (2010). European security and defense policy: From taboo to a spearhead of EU foreign policy. In F. Bindi (Ed.), *The foreign policy of the European Union: Assessing Europe's role in the world.* Washington, DC: Brookings Institution Press.

Kirchner, E. (2006). The challenge of European Union security governance. *Journal of Common Market Studies, 44*(5), 947–968.

Kølvraa, Ch. (2010). *Imagining Europe as a global player: The ideological construction of a New European identity within the EU.* Bruxelles: P.I.E. Peter Lang.

Kurowska, X. (2008). The role of ESDP operations. In M. Merlingen & R. Ostrauskaite (Eds.), *The European security and defence policy: Implementation perspective.* London/New York: Routledge.

Longo, F. (2010). Justice and home affairs as a new tool of European foreign policy. In F. Bindi (Ed.), *The foreign policy of the European Union: Assessing Europe's role in the world.* Washington, DC: Brookings Institution Press.

Matlary, J. H. (2009). *European Union security dynamics in the new national interest.* Basingstoke/New York: Palgrave Macmillan.

Mattelaer, A., & Coelmont, J. (2013). Modern European operations: From Phoney Wars to sickle cuts. In S. Biscop & D. Fiott (Eds.), *The state of defence in Europe: State of emergency?* Egmont Paper No. 62. Gent: Academia Press.

Merlingen, M., & Ostrauskaite, R. (2008). The implementation of the ESDP: Issues and tentative generalizations. In M. Merlingen & R. Ostrauskaite (Eds.), *The European security and defence policy: Implementation perspective*. London/New York: Routledge.

Müller-Wille, B. (2004). *For our eyes only? Shaping an intelligence community within the EU*. Occasional Papers no. 50. Paris: EU Institute for Security Studies

Müller-Wille, B. (2008). The effect of international terrorism on EU intelligence cooperation. *Journal of Common Market Studies, 46*(1), 49–73.

Nomikos, J. (2014). European Union Intelligence Analysis Centre (INTCEN): Next stop to an agency? *Journal of Mediterranean and Balkan Intelligence, 4*(2), 5–13.

Oberson, F. (1998). Intelligence cooperation in Europe: The WEU intelligence section and situation centre. In A. Politi (Ed.), *Towards a European intelligence policy*. Chaillot Paper no. 34. Paris: Institute for Security Studies of the WEU.

Pasco, X. (2004). Ready for take-off? European defence and space technology. In C. Bildt, M. Dillon, D. Keohane, X. Pasco, & T. Valasek (Eds.), *Europe in space*. London: Centre for European Reform.

Payne, T. (2010). The European External Action Service and the EU Military Staff. *Impetus. Bulletin of the EU Military Staff, 9*, 10–11.

Robinson, N., & Gaspers, J. (2014). *Information security and data protection legal and policy frameworks applicable to European Union institutions and agencies*. Santa Monica: RAND Corporation.

Rolington, A. (2013). *Strategic intelligence for the 21st century. The mosaic method*. Oxford: Oxford University Press.

Smith, M. E. (2004b). *Europe's foreign and security policy. The institutionalization of cooperation*. Cambridge: Cambridge University Press.

Svendsen, A. D. M. (2010). *Intelligence cooperation and the war on terror. Anglo-American security relations after 9/11*. Abingdon/New York: Routledge.

Thym, D. (2011). The intergovernmental constitution of the EU's foreign, security & defence executive. *European Constitutional Law Review, 7*(3), 453–480.

Trybus, M. (2005). *European Union law and defence integration*. Oxford/Portland: Hart Publishing.

Utley, R. E. (2012). At war with Al Qaeda: France and international terrorism, 2001–11. In R. E. Utley (Ed.), *9/11 ten years after: Perspectives and problems*. Farnham/Burlington: Ashgate.

Van Osch, T. (2013). Positive trend will continue. *Impetus. Bulletin of the EU Military Staff*, 15, 2–4.

Van Vooren, B. (2011). A legal-institutional perspective on the European External Action Service. *Common Market Law Review, 48*(2), 475–502.

Vaz Antunes, J. N. J. (2005). European Union Military Staff's Intelligence Division. Developing an intelligence capability: The European Union. *Studies in Intelligence, 49*(4), 65–70.

Walsh, J. I. (2009, April). Security Policy and Intelligence Cooperation in the European Union. Paper prepared for the biennial meeting of the European Union Studies Association, Los Angeles. At http://www.euce.org/eusa2009/papers/walsh_12C.pdf. Accessed 14 May 2012.

WEU (1995a, November 14). *European Security: A Common Concept of the 27 WEU Countries.* Extraordinary Council of Ministers, Madrid. At http://www.bits.de/NRANEU/docs/WEU141195.PDF. Accessed 17 Apr 2012.

WEU (1995b, May 15). *Lisbon Declaration. WEU Council of Ministers.* At http://www.weu.int/documents/950515en.pdf. Accessed 17 Apr 2012.

Whitman, R. (2006). Muscles from Brussels: The demise of civilian power Europe? In O. Elgström & M. Smith (Eds.), *The European Union's roles in international politics. Concepts and analysis.* London/New York: Routledge.

Zwolski, K. (2009). The European Union as a security actor: Moving beyond the second pillar. *Journal of Contemporary European Research, 5*(1), 82–96.

Zwolski, K. (2012). The EU as an international security actor after Lisbon: Finally a green light for a holistic approach? *Cooperation and Conflict, 47*(1), 68–87.

CHAPTER 5

Situational Intelligence and Early Warning

Intelligence security in the European Union seeks to support the efforts of its institutions and Member States to mitigate the impact of crises, natural catastrophes and man-made disasters, using its situational-awareness and early warning capabilities. Both institutions and individual states seek to produce an appropriate response to transborder crises and emergencies affecting the EU, though often originating far from the territory of its Member States. The scale and speed of crisis proliferation is one of the biggest challenges for modern states and international organisations. Not only must they address the root causes and catalysts of a crisis or an emergency, but they also have to prepare themselves to confront its direct consequences and far-reaching repercussions for the stability, security and well-being of their nation. Therefore, they need to establish a comprehensive early warning and crisis-response system based on inter-governmental cooperation and cross-border coordination. The ability to identify, assess and make sense of a crisis is tremendously important in contemporary crisis-management methodology (Baumard 1994, p. 30; Fishbein and Treverton 2004; Boin et al. 2005, Chap. 2; Houben 2005, pp. 3–11; Klein et al. 2006, pp. 71–2; Aven and Renn 2010; Fishbein 2011; Moore 2011; Simonović 2011; Boin et al. 2014, pp. 13–6; Post 2015).

Developments at the turn of the twenty-first century and since have had a tremendous impact on the organisation and functioning of the EU crisis-management system. Natural disasters, social revolutions and persistent sources of instability have characterised the new security environment.

A. Gruszczak, *Intelligence Security in the European Union*,
DOI 10.1057/978-1-137-45512-3_5

Floods in Pakistan, the earthquake in Haiti, volcanic ash over Iceland, the Arab Spring and the 'Fire in the East' (annexation of the Crimea by Russia, separatist armed movements in eastern Ukraine, the emergence of the Islamic State, protracted civil war in Syria) have been the most telling examples of high-risk crisis situations demanding a prompt, effective and long-lasting response from the international community and global actors involved in crisis management and stabilisation in the areas of natural disasters, civil unrest and political breakdown. Moreover, events in many of these 'hot spots' have had almost immediate consequences for the borders, territories and societies of the EU. Successive waves of irregular migration from North Africa, the Middle East and the Balkans, hosts of asylum seekers storming reception centres in EU Member States, and the dangerous phenomenon of 'foreign fighters' linked to the Islamic State are the most striking examples of how external crises reach far beyond their immediate environs to bring about serious negative consequences for the EU. Moreover, the direct negative effects of external crises may produce long-term structural changes in political, societal and even legal systems. For instance, the repercussions of the Arab Spring, civil wars in Iraq and Syria, state failure in several African countries and the hybrid war in eastern Ukraine have put increasing pressure on the Schengen regime and contributed to the revision and modification of the principle of the free movement of persons (Brady 2012; Peers 2013; Zaiotti 2013; Cornelisse 2014).

As we saw in Chap. 4, the military intelligence hub that emerged in response to political, institutional and legal changes in the EU's security policies authorised Member States to launch military operations in fulfilment of the Petersberg tasks. Crisis management and early warning were considered part of the European Security and Defence Policy, mostly due to the 'expeditionary' dimension of civilian and military crisis-management capabilities. Since the 2003 police mission in Bosnia and Herzegovina, the first ever EU-led intervention, the EU and Member States have been seeking the most appropriate ways of ensuring the effectiveness of their efforts. Missions and operations under the CSDP have changed over time, due to enlargement of the scope of engagement, availability of resources and tools, and variety of methods of their realisation.

Anticipating the content of Chaps. 6 and 7, it is fair to say that elements of early warning and crisis prevention can be found in both CFSP and JHA cooperation. Socio-cultural intelligence, which supports the EU's diplomacy and external relations, collects and analyses a large amount of data and information about crises, disruptions, emergencies and hazards occurring outside the European Union yet having a considerable, often serious or negative, impact on EU policy, identity or security. The protection and safety of EU citizens, as well as representatives or officials of EU institutions and agencies, is no less important. Equally significant are crime prevention and law enforcement. Exogenous threats like terrorism, organised crime, illegal migration or cyber-attacks have to be anticipated and if possible prevented. Hence, the internal security hub, though focused on criminal intelligence analysis, also involves elements of situational intelligence acquired from early warning systems and strategic assessment mechanisms.

At both functional and institutional levels, however, the EU fails to relate fully to this vast area of crisis management. The introduction and development of some elements of situational intelligence have generated the crisis-management hub as a network structure linking the institutions, units, procedures and mechanisms involved in early warning, early response, contingency planning and strategic forecast. National prejudices, legal boundaries, bureaucratic barriers and institutional arrangements, however, are such that the EU crisis-management hub remains a loose nodal configuration of units and services connected by strong links to EU civilian crisis-management mechanisms and more loosely connected to transborder crisis procedures and national emergency systems.

Crisis Management and Situational Intelligence in the EU

Managing crises and emergencies is a challenging and demanding task for any local, regional, national or international authority in charge of risk prevention, the mitigation of disasters, civil protection, crisis recovery and reconstruction, or infrastructure protection. Since the European Union embarked on constructing a 'protection space' (Boin et al. 2006; Rhinard et al. 2006; Boin et al. 2013; Post 2015), the notion of crisis management has been thoroughly discussed and is regarded by some scholars as a new type of policy activity at the EU level (Duke 2002; Porfiriev 2005; Boin et al. 2006, p. 406; Ekengren and Groenleer 2006; Blockmans 2008; Gross 2009, pp. 171–2; Larsson et al. 2009, pp. 1–2; Major and Bail 2011, pp. 15–17; Gebhard and Norheim-Martinsen 2011, pp. 231–6; Morsut 2014). As noted above, an all-encompassing approach to EU crisis management is not feasible in either the functional, political or institutional senses. So, tackling the issue of crisis prevention and early warning in the crisis-management hub requires the concept of crisis management in the EU to be clarified in view of the presumed implementation of the situational intelligence approach.

Miozzo and Missiroli (2014, p. 5) point out the important distinction in EU security policies between the notion and the practical meaning of the term 'crisis management'. First, crisis management can be identified with 'expeditionary' (out-of-EU) civilian missions and military operations under the CSDP. Second, crisis management includes 'response schemes in the fields of peace-building, security sector reform, support to governance, trans-regional threats, emerging or acute crisis situations, CBRN risk mitigation, and pre/post-crisis capacity building'. However, these authors omit internal aspects of crisis management within EU Member States. The present analysis follows the crisis types identified by Boin, Rhinard and Ekengren, who distinguished three types of crisis situation eliciting a possible (legally and politically feasible) response from the EU and its members (Boin et al. 2013, pp. 7–10).

Type I is the national crisis; type II the external crisis; and type III is the transborder crisis. In the first case, the EU's capabilities can be used within the framework of the Civil Protection Mechanism, which fosters cooperation between national civil protection authorities across Europe and provides assistance in the immediate aftermath of a catastrophe or disaster, though it is not applied in the fields of health, justice and home affairs. The mechanism can be activated in response to disasters occurring both within and outside the European Union. In practice, requests for assistance relatively seldom come from EU Member States. The type II situation is commonly identified with EU crisis-management capabilities and mechanisms. It invokes both military responses through CSDP operations conducted under the EU military command and control, and civilian aspects of crisis management outside the EU. The involvement of military intelligence in CSDP operations has already been elaborated in Chap. 4. Situational intelligence in support of civilian capabilities in CSDP missions draws on dedicated functional and institutional arrangements developed in the course of military and civilian crisis management. Such solutions have resulted in an expanded nodal structure aggregating existing institutionalised forms of EU crisis management and improving circulation of information and analysis.

The third type of crisis situation is produced by the transborder effects of deterritorialised risks and threats proliferating across the borders of

EU Member States. They demand a collective response since their source can be neither physically located nor immediately neutralised. The consequences and depth of a crisis affect multiple actors at different levels of territorial and administrative authority. Boin, Ekengren and Rhinard give several examples of such threats: epidemics, extreme weather events, cyber-attacks, the proliferation of chemical and biological weapons, and unexpected refugee flows (Boin et al. 2013, pp. 9–10).

Another EU instrument for managing transborder crises is the 'solidarity clause' enshrined in Article 222 TFEU (Myrdal and Rhinard 2010; von Ondarza and Parkes 2010; Ferreira-Pereira and Groom 2010; Fuchs-Drapier 2011; Hatzigeorgopoulos 2012). This provides for a coordinated response from the EU to disasters, terrorist attacks and non-military crises emerging within the territory of Member States. It has not been applied yet and the implementation arrangements have not been finalised.

Member States are exposed to the whole array of threats, hazards, and natural and man-made disasters constituting potential crises and emergencies that demand a resolute, immediate and effective response from their own authorities assisted by relevant EU institutions and mechanisms. Any decision making in this regard requires solid, professional and effective intelligence support focused on early warning and situational assessments.

The present book, which observes and analyses crisis-management mechanisms from the precautionary perspective, assumes that actors engaged in the effective management and mitigation of a crisis need to activate crisis-prevention mechanisms coupled to early warning. The latter means 'any initiative that focuses on systematic data collection, analysis and/or formulation of recommendations, including risk assessment and information sharing, regardless of topic, whether they are quantitative, qualitative or a blend of both' (Austin 2004, p. 2). The EU's early warning and crisis response has been characterised by a complex multi-level institutional configuration addressing a wide range of crisis-prone areas and risk sources, and by loose connectivity among the host of actors involved. As a result, horizontal cross-field communication channels at the EU level enable only to a certain degree the collation, comparison, analysis and processing of selected information from scattered sources belonging to particular segments of the EU crisis-management hub. Different levels of decision making and responsibility in the EU have created a polycentric setting around the institutions, agencies, roles, mechanisms and tools involved in early warning and crisis response.

To overcome theoretical flaws and practical problems, this book takes a generic approach to situational intelligence in the field of crisis management in the EU. According to Claudia Dent, situational intelligence is critical during a crisis and equally relevant to crisis prevention (Dent 2013). It can present a multidimensional set of information that looks at risks and opportunities comprehensively, allowing consideration of many options for crisis management and mitigation (Di Stasio 2015). The situational intelligence developed by relevant EU bodies tends to link, coordinate and fuse scattered information and analytical materials to produce a relatively comprehensive picture of ongoing processes and future developments. It is, however, strongly predetermined by political principles and institutional limitations, which in effect preclude the emergence of a functional/institutional core. So, despite the relatively consolidated crisis-management capabilities of the CSDP, the European Union has not yet taken on Member States' role of 'crisis manager'. It continues to rely on national foreign policy responses to international and regional crises (Gross 2009, p. xi). While this implies a vertical, bottom-up, Member States-led architecture of intelligence support for crisis management, the situational intelligence approach enables a vertical configuration for early warning and crisis-prevention arrangements, worked out by various stakeholders within the EU's functional and institutional framework.

Situational intelligence and early warning entail anticipatory measures. Situational intelligence, though based on 'soft' capabilities (Mounier 2009a, p. 50), requires shared analysis of the causes of a potential conflict or crisis, the indigenous actors and external participants in the crisis area, and the dynamics, potential risks and dangers of the situation. As an ingredient of early warning, it not only reduces uncertainty, but also provides scenarios and options for decision makers (Ricci 2014, p. 188). For many years the European Union has been developing a coordinated approach to crisis situations, conflicts and disasters, seeking to improve its organisational and technical resources, and capacity to handle large-scale global emergencies and crises, as well as local and regional sources of conflict, tension and instability. The embryonic forms of situational intelligence cooperation emerged within the Western European Union and addressed external crises, conflicts and emergencies under the Petersberg tasks. In June 1997 the European Council called for an early warning unit within the CFSP, acknowledging the need for Member States and the Commission to provide the confidential information necessary to assist the policy-planning process (European Council 1997; Council of the EU 2001b). A Policy Planning and Early Warning Unit established in the General Secretariat of the Council was tasked with ‘providing timely assessments and early warning of events or situations which may have significant repercussions for the Union’s foreign and security policy, including potential political crises’ (European Union 1997a, p. 132). Interestingly, the Declaration of the Western European Union on its role and its relations with the European Union and with the Atlantic Alliance, attached to the Treaty of Amsterdam, provided that the EU Policy Planning and Early Warning Unit could draw on the resources of the WEU’s Planning Cell, Situation Centre and Satellite Centre (European Union 1997b, pp. 129–31).

The development of the European Security and Defence Policy as a result of decisions taken by heads of Member States and governments in 1998–1999 was focused on military and civilian capabilities (Giegerich 2010, pp. 42–50). The events of 9/11 and the subsequent shift in EU security policy and strategy towards counter-terrorism and civil protection fostered the development of crisis-management cooperation in the European Union. Early warning systems and elements of situational intelligence had grown spontaneously but without appropriate cross-sectoral coordination and at different levels of organisational and technical advancement (Olsson and Larsson 2009, p. 165). The launch of the first ESDP missions coincided with the mounting terrorist threat that culminated in the Madrid and London bombings of 2004 and 2005. These events triggered discussions on how to improve coordination within the Commission and between this institution and the General Secretariat of the Council, particularly the High Representative for CFSP. Despite the creation of new mechanisms for collection, analysis and sharing of information on crisis and conflict parameters, crisis-management schemes were not significantly improved.

As we saw in Chap. 4, INTCEN had been established in 2002 as the Joint Situation Centre responsible for monitoring the security landscape and preparing situation assessments, especially in the field of European security and defence policy and during crisis-management operations. SITCEN was tasked with contributing to the early warning work of the Council and the High Representative, giving specialised back-up to crisis task forces requiring intelligence and situational awareness and providing support for the Council and the High Representative during the preparation and conduct of crisis-management operations (European Parliament 2009; House of Lords 2003, p.25). The Centre collected and processed information on the background and development of crisis situations, reporting to the High Representative and relevant EU bodies, especially the Political and Security Committee (PSC) and the EU Military Committee. It could be asked by the PSC to provide specific reports contributing to a further analysis of a crisis (Council of the EU 2003a, pp. 7–8). SITCEN was expected to deliver detailed intelligence products rather than policy guidelines or anti-terrorist blueprints for EU institutions or national governments (Duke 2006, p. 618). It contributed, along with EUMS and the Directorate-General for External Relations (RELEX) of the European Commission, to a confidential early warning document called 'the Watchlist', listing states the EU ought to monitor closely in the context of possible crises or proliferated threats. The Watchlist was updated half-yearly (once per presidency), making use of available intelligence, cluster analysis and cross-checked quantitative data as well as situation assessments that mostly explored qualitative indicators but also made considerable use of OSINT. Countries on the list were prioritised according to the likelihood of a crisis and its possible impact on the EU (Council of the EU 2007a, p. 72; 2010a, p. 58; Shapcott 2011, p. 119; Hemmer and Smits 2011, p. 10).

Following the Lisbon treaty reform, the Centre maintained its auxiliary role in EU crisis-management policy. One of its main objectives was to provide specialised analytical back-up to crisis task forces requiring intelligence and situational awareness for their field activities as well as intelligence support for the Council and the High Representative during the preparation and conduct of crisis-management operations.

The Web-based rapid alert system ARGUS was created in 2006 to ensure swift information exchange between the Commission's various Directorates-General and better coordinate its response capacity during major cross-sectoral crises. ARGUS brought together all relevant Commission services so as to coordinate response efforts, circulate non-classified information and evaluate the best options for an effective response to an emergency (Zandén Kjellén 2009, pp. 77–8). Another important application was the EU Emergency Crisis Co-ordination Arrangements (CCA) approved by the Council of the EU in June 2006. This scheme was established with a view to the provision of rapid and coordinated EU horizontal policy responses in a serious crisis situation. The CCA enabled Member States, through their permanent representatives in Brussels, to exchange information and coordinate actions in an emergency or an extremely serious crisis situation affecting several

Member States (Larsson 2009, pp. 127–30). SITCEN was also engaged in the CCA. Johnny Engell-Hansen, the former Head of the Operations Unit at SITCEN, explained that the Centre's role was 'to provide the main operational and infrastructural backbone for supporting the EU Presidency and Member States in implementing these CCA arrangements in a crisis situation' (House of Lords 2009, p. 32).

Communication between relevant departments within the Commission and between the EU and Member States was improved thanks to the creation of the Community Civil Protection Mechanism. The mechanism provided for the development of detection and early warning systems for disasters potentially affecting the territory of Member States. This task was mandated to the new Monitoring and Information Centre (MIC), accessible 24/7 for Member States and the Commission, and designed to provide timely and effective information ensuring preparedness for an effective response (Morsut 2014, pp. 143–9).

The Lisbon treaty heralded a significant change in the EU's crisis-management system, particularly concerning the tendency to concentrate the relevant elements and capabilities within the EEAS. Despite the mushrooming of crisis-management arrangements across the Commission and within the Council, there had been 'no common EU-wide understanding of early warning and early response for conflict prevention' (Beswick 2012, p. 8), Europeans witnessed a series of catastrophes, emergencies, conflicts and crises: the Haiti earthquake in 2010; ash cloud problems caused by the eruption of the volcano Eyjafjallajökull in Iceland in 2010; the nuclear accident at the Fukushima plant in 2011; the H1N1 and H5N1 influenza virus pandemics of 2009; floods in Central Europe; and the outbreak of civil war in Syria.

The High Representative, Catherine Ashton, decided to build up crisis-response capabilities within EEAS and concentrate them in the Crisis Response and Operational Co-ordination Department. Political backing was granted by the Council which in its conclusions on conflict prevention adopted on 20 June 2011 stated that 'early warning needs to be further strengthened within the EU, by better integrating existing early warning capacities and outputs from all sources, including from Member States, and drawing more extensively upon field-based information from EU Delegations and civil society actors, in order to provide a more solid foundation for conflict risk analysis. Enhancing early warning will also enable the EU to work more effectively with partners regarding responsibility to protect and the protection of human rights' (Council of the

EU 2011d, p. 3). Ministers also acknowledged that there was still a realistic option for preventive action, subject to Member States' capacity to agree on and implement coherent, viable and practical mechanisms. They noted that 'More emphasis also needs to be put on taking early action, to mitigate the risks of outbreak and recurrence of conflicts, for example through the effective utilization of conflict risk analysis' (Council of the EU 2011d, p. 4).

Despite the reform of the crisis-management hub in 2012, this area remained fragmented and its institutional components were unevenly developed and insufficiently flexible. On the initiative of High Representative Ashton, a comprehensive approach to complex crisis response was presented in a joint communication to the European Parliament and the Council in December 2013 (High Representative 2013). It highlighted the requirement for a proper understanding of all stages of the cycle of conflict or other external crises, to ensure early warning and preparedness for crisis response and management. As a result, the EU should develop a shared analysis approach by better connecting the existing institutional services and facilitating early, proactive and regular information and intelligence sharing. The existing institutional and working arrangements, involving both Member States and dedicated EU services, units and teams, should be gradually improved to focus on tailored analysis and assessment built on all available information and knowledge (High Representative 2013, p. 5).

Although the shared understanding of security needs and possibilities underpinning the rationale for EU cooperation and integration of security policies and fields seemed to be at the core of the comprehensive approach, it has not proved efficient enough to respond to the whole spectrum of crisis-management tasks and objectives (Mölling 2008; Drent 2011, pp. 5–6). Cooperation problems between the military intelligence hub (except for elements delivering intelligence products within the SIAC framework) and the crisis-management hub has been one of the visible obstacles to enhanced coordination between civilian and military EEAS elements (Adebahr 2011, pp. 5–7). Institutional and functional divisions have also been clearly visible in the field of civil protection. For instance, efforts by Ashton to merge the EU Situation Room and the Emergency Response Coordination Centre (formerly the Monitoring and Information Centre) within the Commission's Humanitarian Aid and Civil Protection Department failed.

The adoption of the EU Integrated Political Crisis Response (IPCR) arrangements in 2013, this time including a solidarity clause, marked a further effort to consolidate the unstable EU crisis-management architecture (Nimark and Pawlak 2014, p. 108). The value it added to the existing patterns of cooperation consisted in 'bring[ing] numerous actors around the same "table": member states, the presidency of the Council, the European Commission and the European External Action Service (EEAS)' (Pawlak 2014, p. 86). The IPCR has also improved the information workflow with the provision of a Web platform as a communication framework.

It is still too early to evaluate the real significance of these changes, especially in terms of the creation of synergies between stakeholders and links between existing information resources and analysis capabilities. It seems, however, that the IPCR-led crisis-management hub is more focused on early warning and proactive information sharing, as well as on support for decision making, seeking to use situational intelligence to a considerably greater extent than was previously the case.

The Organisation and Coordination of the EU Crisis-Management Hub

The EU crisis-management hub is populated with numerous EU institutions, units and bodies engaged in crisis detection, including early warning, monitoring, sounding the alarm and responding to a crisis situation. However, the majority of their 'sense-making' systems and instruments have been established and launched at the operational level. They are charged with preparing an immediate response to an existing crisis and then monitoring ongoing developments in order to provide updated assessment and warning. Only a few of them are strictly devoted to precautionary information management, focusing on gathering, correlating and analysing data and information for preparedness and capacity building, and creating situational awareness at the strategic level. This task is in part accomplished within the military intelligence hub, especially in matters concerning CSDP missions and operations and strategic forecasts on 'hard' security threats. Crisis detection, early warning and situational intelligence apply to numerous aspects of 'soft' security, such as civil protection, human security, the rule of law or political stability.

The creation of the EU crisis-management hub was motivated by strategic and political factors. The 2010 changes that concentrated early warning and crisis management in EEAS produced important consequences. The crisis-management system was focused on external actions under CFSP and CSDP, but the political imperative of the comprehensive approach required a more agile and adaptable solution that properly addressed the need to operate at different levels of crisis response. While response and follow-up organisation (prevention, recovery, stabilisation) was relatively effective, the early warning and awareness-building mechanisms and tools demanded a broader and more flexible arrangement, capable of combining and integrating various widely dispersed methods and tools. The Department for Crisis Response and Operational Coordination (MD VII) within the EEAS consolidated organisational and human resources around all-source analytical capabilities. As a result, the crisis-management hub has acquired a multi-level architecture, with the IPCR as a kind of 'superstructure' and MD VII as a coordinator for external crises, activating, managing and monitoring the Crisis Response System but also cooperating with relevant EEAS units or relatively autonomous dedicated agencies, such as INTCEN, EUMS or SATCEN.

The Crisis Response and Operational Co-ordination Department was intended to mobilise and engage EU institutions and Member States to effectively manage civilian crises and emergencies, creating situational awareness among EU-wide actors through strategic assessment and ensuring coherence of policies and actions (see EEAS 2014a). The Department's establishment, however, was characterised by personal motives. According to EEAS officials,[1] High Representative Catherine Ashton saw a strong candidate for its head in Agostino Miozzo, an Italian official with experience in disaster management and emergency relief. Smith (2013a, p. 1309) wrote that 'In fact, the position of EEAS Managing Director for Crisis Response and Operational Co-ordination was created by Ashton so that Miozzo could hold it'. Another reflection, shared by an EEAS official,[2] was that the HR/VP sought to 'kill three birds with one stone': improve EU civilian crisis management, especially in the aftermath of the Haiti earthquake of January 2010, when the EU's limited response was openly and bitterly criticised (Ashton 2014, p. 12); strengthen the crisis-response unit in EEAS, with its militarised institutional structure; and establish an experienced, strong and loyal partner at the head of the unit (see also Tercovich 2014, p. 152). Miozzo as Managing Director reported to the HR/VP but had no direct links to the military segment in EEAS;[3] he was thus in an exceptionally strong position compared with other EEAS bodies in charge of crisis management.

MD VII is responsible for the activation of the Crisis Response System (CRS), which encompasses the Crisis Management Board, the EU Situation Room and the Crisis Platform, one of its main priorities being information sharing. The CRS was formed in 2011, when growing instability in North Africa, the Middle East, Western Africa, South Asia, and Central America and the Caribbean made it desirable to pool EU resources and support political decision making in respect of emerging or enduring crises. Its role is to implement standard procedures to tackle crises and tensions outside the EU, or those generated inside the Union by external drivers, which may affect EU security interests. In particular, it seeks to deal with crises affecting EU delegations, or any other EU assets or persons in a third country. The CRS' competences range 'from prevention and preparedness to response and recovery aiming to achieve a comprehensive EU crisis response and management capability' (EEAS 2014b).

The EU Situation Room (SitRoom) is 'the first point of contact for all information on crisis situations' (EEAS 2014c). It is the only 24/7 capability at EU level, acting as a permanent switchboard for EEAS and the European Commission, and delivering accurate and up-to-date crisis-related information to decision makers. It selects, collates and verifies information from all available sources, including open sources, EU delegations, Member States, EU CSDP operations and missions, EU Special Representatives' teams, EEAS exploratory missions, and relevant international organisations (Nimark and Pawlak 2014, pp. 112–3). Its task was defined as follows: 'to lead, manage and develop all EEAS permanence and situational awareness capabilities' (High Representative 2011).

According to the Council of the EU, the Situation Room complements the analytical work of INTCEN and EUMS INT within the SIAC format (Council of the EU 2012a, p. 92). The SitRoom's role is to support decision making. It does not deliver intelligence products, but it prepares monitoring materials and situational reports, such as daily briefings on world affairs, press reviews for EU delegations, situation reports for active EU Crisis Platforms and crisis-response factsheets (Manchin 2014, pp. 167–8). In 2014, it handed over more than 650 reporting and monitoring products (High Representative 2015, pp. 10–11).The Situation Room also houses the Watch-Keeping Capability (WKC), a 24/7 desk operated by a dozen police and military officers tasked with ensuring a fast, continuous and systematic flow of specific information related to ongoing CSDP missions and operations. Although significant for early warning, it is not designed to provide intelligence (Beswick 2012, p. 8; Ceuterick and Weston 2012, p. 23).

The EU Crisis Platform is the second important element of the CRS. It is an ad hoc undertaking activated and chaired by the HR/VP within the institutional framework of EEAS and connected with relevant Commission services and the General Secretariat of the Council. It aims to provide an adequate and timely response, in strategic, political and analytical terms, to external crises requiring coordinated action at EU level. It seeks to facilitate information sharing during all phases of an ongoing crisis, collecting, processing and disseminating information and analyses on the most relevant aspects of a given crisis situation, including political, economic, social, military and humanitarian issues, and the international environment. The Crisis Platform enables EU officials and invited national experts to access well-ordered and streamlined knowledge and to keep information circulating among different institutional stakeholders. It can also offer first-hand information and accounts obtained by EU exploratory or fact-finding missions (as in the case of the 2011 Libyan revolt). Between March and October 2011 the Platform was convened 14 times (Koenig 2014, p. 168), and by the end of 2014 it had responded to crisis situations in Mali, DR Congo, Libya, Syria, the Ivory Coast, the Sahel, the Horn of Africa, Kenya, Lebanon, South Sudan and Myanmar (Council of the EU 2014d). The meetings kept information flowing among the different units involved, especially those dealing with humanitarian issues, security problems and political developments in Libya (Council of the EU 2012a, p. 105). The Libya Crisis Platform was especially relevant due to the dynamic of the internal conflict, the NATO-led military intervention, the grave humanitarian repercussions of the civil war and potentially direct negative outcomes for the EU and some of its Member States (Tercovich 2014, p. 154; Council of the EU 2012a, p. 105).

Situational Intelligence Workflow in the Crisis-Management Hub

Since the revision of crisis coordination in 2013, data collection, analysis and distribution have taken place within the framework of the EU Integrated Political Crisis Response (IPCR). This took over from the preceding Crisis Co-ordination Arrangements the duties of drawing attention to and monitoring unfolding crisis situations, sharing and distributing related information and contacting the relevant EEAS services and the General Secretariat of the Council. The Presidency of the Council plays a central role in all stages of the IPCR arrangements (Council of the EU 2013, p. 6). To facilitate information workflow and strengthen the comprehensive approach to crisis management, the Commission and the EEAS decided to develop an Integrated Situational Awareness and Analysis component (ISAA). ISAA is a key information-sharing capability under the IPCR arrangements, aggregating inputs from Member States and integrating them with existing information, and using the existing capabilities of the Commission and EEAS (Nimark and Pawlak 2014, p. 112). Its collection and analysis of situational information provides an up-to-date common situational picture to the presidency and supports the Council's decision making (Council of the EU 2014a). When the solidarity clause is invoked, ISAA reports provide a strategic overview of a crisis situation.[4]

Situational intelligence addresses various sources of risks, threats and security concerns located on different layers of political, societal, economic and cultural structures. Identifying and mapping these sources at the EU level is the task of numerous agencies and units with different means and tools at their disposal, as well as capabilities to access, acquire and transmit relevant information and data. We noted in Chap. 4 that classified information owned by national intelligence services of Member States, generally in connection with EU-led military operations, is relatively seldom made available to EU agencies and units. The main reasons are the lack of a proper communication infrastructure and controversies over appropriate personal security clearance. Some classified information is delivered to INTCEN for strategic analyses tackling the major security issues, such as terrorism, WMD proliferation, and illegal arms trading. However, as the former head of the Crisis Room at DG RELEX Andrea Ricci (2014, pp. 192–3) confirms, 'Practice shows that secret intelligence and/or classified information is not necessarily available in the acute phases of a crisis. This may happen because of a "strategic surprise"(failure of early warning processes); because collection assets cannot be redeployed in a new theatre fast enough to provide "just-in-time" intelligence; or because regulation framing the use of secret intelligence slows down transmission enough to force crisis responders to seek answers by alternative means.'

The vast area of crisis management in which situational intelligence is applied coincides with a wide, diversified and fragmented communication and IT architecture. Information workflow is concentrated in functional/institutional nodes linked up to the IPCR Web Platform. This loose arrangement reflects the political and operational constraints which have determined the overall functionality of the crisis-management hub.

Regardless of the considerable doubts and reservations raised by some EU officials and representatives of Member States, the crisis-management hub makes extensive use of open sources. In the early 2000s the European Commission developed an open-source intelligence platform to integrate and effectively explore scattered sources. It was called Tarîqa and was destined for the Crisis Platform and Policy Co-ordination at the Directorate-General for External Relations (DG RELEX). Originally, it provided real-time support for early warning and situational awareness, enabling EU delegations around the world to follow global developments from a single integrated source of information stored in a multimedia content database (Stauffacher et al. 2005, p. 21). Over time, it became available to more than a thousand officials (Landaburu 2008, p. 70). With the changes brought about by the Lisbon treaty, Tarîqa was upgraded in 2011 to its 3.0 version and transferred to EEAS (Duke 2014, p. 248). As an internal Web application, it is deployed in the EU Situation Room through an encrypted SSL connection (Tarîqa 2012, p. 8). It offers advanced information retrieval tools, available through a user-friendly interface. Supported by a multimedia content database, it facilitates the search, analysis and retrieval of useful knowledge from a vast number of unclassified information sources. These include full-text databases, audio-visual material, satellite imagery, declassified military maps, internal news feeds and publications. Searches automatically filter quantitative and qualitative data from media news, RSS feeds, Internet search engines, open websites and social media, geospatial information systems and commercial subscription databases (such as Lexis Nexis, Oxford Analytica, Factiva, IHS Jane's), as well as information from the Commission and other relevant EU agencies and units (Babaud and Mirimanova 2011, p. 13). Authorised users may send pre-defined requests, regularly updated by the system manager, or their own queries. In return, they get information which is automatically filtered and ranked in terms of relevance (Tarîqa 2012, p. 8). Tarîqa uses only primary sources and is focused on testimonials, documentaries and investigative journalism. It also values knowledge obtained from the EU's diplomatic community as well as exclusive, scarcely available resources (Banim 2006, p. 274).

Another, and more advanced, tool of information gathering and analysis based on open sources is the Online Data and Information Network system, developed by the EU's Joint Research Centre. Its filtering and extraction engines enable the application of more precise keywords, making it better tailored to user needs (Beswick 2012, p. 8).

For the purposes of situational assessment and crisis detection, geospatial imagery and intelligence may be provided on request by the EU Satellite Centre. At the crisis-detection stage, the Centre can be tasked by the High Representative with monitoring the identified crisis (Council of the EU 2003a, p. 8). SATCEN also participates in exercises to verify the appropriateness and viability of crisis-management procedures at EU level and contribute to their further development and streamlining (EUSC 2015, p. 16).

An interesting and relatively recent geospatial solution in civilian emergency management is the Copernicus programme, launched in 2014 and designed to ensure autonomous capacity for space-borne observations. It will provide emergency response information in relation to different types of disasters as well as prevention, preparedness, response and recovery activities. It will also support civil security activities in Europe, improving crisis prevention, preparedness and response capacities with special reference to border and maritime surveillance, and the EU's external activities to the extent allowed by the Commission (European Parliament and the Council of the EU 2014d, p. 53). Practical support in a disaster response situation is illustrated by the Copernicus Emergency Management Service mapping (Copernicus 2014). This was first used in connection with Typhoon Haiyan's landfall in the Philippines in 2013, producing annotated maps for the rescue operation (Dietrich and Pawlak 2014, p. 135).

The situational intelligence cycle is driven by the presidency upon request and with approval from Member States acting through COREPER. A decision taken in the IPCR activates ISAA capabilities, initiating information analysis and sharing mechanisms via the IPCR Web Platform, which links mechanisms and tools developed by the relevant units within the Commission, the EEAS (especially INTCEN), the Council (including Counter-Terrorism Coordinator, if necessary) and Member States. Core users delegate contact persons to handle the flow of information and Member States maintain points of contact at a national level (EEAS 2013a).

ISAA's ability to deliver a shared situational picture relies on existing situational intelligence arrangements and the capabilities of the Commission and EEAS. Since the IPCR Web Platform does not replace any of the existing sectoral Web tools, it can retrieve relevant materials subject to validation by a managing authority. They can be complemented by other existing channels for sharing information classified above 'EU Restricted', especially those linking Member States' information and intelligence resources (Council of the EU 2014a).

Most background information and strategic assessments reach the EU Situation Room. This unit alerts EEAS, the Commission, the GSC and Member States to risks and dangers posed by an emerging crisis situation, contributing at the same time with tailor-made situational reports made up of validated inputs from the available stakeholders on a voluntary basis (Council of the EU 2014b). SitRoom's own analysis tools support such functionalities as cluster analysis, with the aim of identifying and examining risk patterns and crisis triggers (Babaud and Mirimanova 2011, p. 12). Where civilian and military aspects of crisis management under CSDP missions are involved, SitRoom may take advantage of its functional liaison with the Watch-Keeping Capability. The WKC acts as the switchboard for external security-related issues and it can improve information exchange and the quality of situational intelligence going to the relevant EEAS actors, and the HR/VP in particular, as well as other stakeholders integrated with the crisis-management hub (Ceuterick and Weston 2012, p. 23).

Information extracted from various sources is streamlined according to its content and destination and uploaded to a dedicated crisis page. Classified information and intelligence concerning crisis management and policy activities in the CSDP domain can be exchanged via the SESAME secure communication system (described in Chap. 4) (DGA 2011, p. 32).

Advantages and Limitations of Early Warning and Situational Intelligence

Strategic intelligence is often understood as a prerequisite of operational activities in the realm of security. The planning, command, conduct and monitoring of crisis-response activities require a proper level of strategic situational awareness and good intelligence support. Preparedness and prevention capacity is no less important for individual safety, public order and the rule of law. The vast security policy area of the European Union makes an integrated, centralised and comprehensive problem-solving approach particularly difficult.

The evolution of the crisis-management hub in the EU has proved that it is difficult to gather up, link and integrate dispersed institutional arrangements, intersected, often overlapping competences, entangled communication channels and scattered information sources. The loose nodal configuration of the parts of the crisis-management hub has been formed in response to an acute need to ensure the effectiveness and viability of the EU early warning and crisis-management systems operating in the spatial, temporal and information domains. Good timing and effective information support are the 'natural' determinants of the stages of effective crisis management. In Patryk Pawlak's apt wording, 'Time and information are among the most valuable commodities during a crisis' (Pawlak 2014, p. 84). Hence, the problem of information management and intelligence support cannot be reduced to the timely activation of crisis procedures and the continuous monitoring of a crisis as it unfolds. Catherine Ashton and her advisers rightly identified this challenge, preparing and subsequently promoting the comprehensive approach. However, a comprehensive and overarching information management and analysis system will not be adequate unless it links up all available information and intelligence sources and integrates organisational, technical and human resources. The mosaic of 'sense-making' systems in the realm of EU crisis management, mapped in detail by Boin, Ekengren and Rhinard (2014), raises an important question about the central role of managing information in respect of a particular crisis (Lennart and Zandee 2014, p. 17). The institutional, as well as political, interplay between the Commission, the EEAS, and the HR/VP and the Council has not yet produced acute turf battles; nonetheless it has too often blurred the boundaries of formal competences and functional settings between particular segments of the crisis-management hub.

The EU as a security community and international actor has taken responsibility for civil protection coordination between Member States, and for civil and military crisis management outside its borders. It has plenty of information sources and has developed a range of mechanisms and tools for the efficient gathering and analysis of data and information referring to threats, risks and security concerns. This has huge potential for the building of accurate, reliable and timely strategic security awareness to underpin early warning mechanisms and crisis-response schemes. The High Representative (2015, pp. 10–11), in the Action Plan on the comprehensive approach, recommended 'enhancing the cooperation via existing mechanism (such as IPCR web platform) which is linking up the various situational awareness and emergency management centres of the Union (Emergency Response Coordination Centre and the EU Situation Room (EU SitRoom) and Member States, as well as EU agencies; further developing practices of exchanging situational reports between above mentioned interlocutors […]'.

The challenge of the integration, cross-referencing and checking of all available information material must be met at the political level, which requires a more open and flexible attitude towards information sharing and intelligence production from EU top officials and representatives of Member States. Situational intelligence in the EU crisis-management hub is a practical solution to the majority of the constraints and shortcomings mentioned, but it cannot be a long-lasting systemic solution to the need for effective and accountable crisis preparedness and response.

Notes

1. Two anonymous EU officials (representing EEAS and the European Commission), interview, June 2012.
2. An anonymous EEAS official, interview, June 2012.
3. High Representative Catherine Ashton confirmed in an answer to the written question from Martin Ehrenhauser, MEP, that 'MD VII does not exchange information with any national intelligence service, neither civilian nor military' (European Parliament 2012b).
4. Article 6, Council Decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause (Council of the EU 2014b).

Bibliography

Adebahr, C. (2011). *The comprehensive approach to crisis management in a concerted Weimar effort*. Genshagener Papiere No. 6. At http://www.stiftung-genshagen.de/fileadmin/Dateien/Publikationen/Genshagener_Papiere/Genshagener_Papiere_2011_06.pdf. Accessed 17 Dec 2013.

Ashton, C. (2014). The role of the European external action service in a global network of crisis room. In P. Pawlak & A. Ricci (Eds.), *Crisis rooms: Towards a global network?* Paris: EU Institute for Security Studies.

Austin, A. (2004). *Early warning and the field: A cargo cult science?* Berlin: Berghof Research Center for Constructive Conflict Management.

Aven, T., & Renn, O. (2010). *Risk management and governance. Concepts guidelines and applications*. Berlin/Heidelberg: Springer-Verlag.

Babaud, S., & Mirimanova, N. (2011). *The European Commission early-warning architecture and crisis-response capacity*. Brussels: IFP-EW/International Alert.

Banim, G. (2006). Early warning for early action. In A. Ricci & E. Kytömaa (Eds.), *Faster and more united? The debate about Europe's crisis response capacity*. Luxembourg: Office for Official Publications of the European Communities.

Baumard, P. (1994). From noticing to making sense: Using intelligence to develop strategy. *International Journal of Intelligence and CounterIntelligence, 7*(1), 29–73.

Beswick, T. (2012). *EU early warning and early response capacity for conflict prevention in the post-Lisbon era*. Brussels: Initiative for Peacebuilding—Early Warning.

Blockmans, S. (Ed.). (2008). *The European Union and crisis management. Policy and legal aspects*. The Hague: T.M.C. Asser Press.

Boin, A., et al. (2005). *The politics of crisis management. Public leadership under pressure*. Cambridge: Cambridge University Press.

Boin, A., Ekengren, M., & Rhinard, M. (2006). Protecting the union: Analysing an emerging policy space. *European Integration, 28*(5), 405–421.

Boin, A., Ekengren, M., & Rhinard, M. (2013). *The European Union as crisis manager. Patterns and prospects*. Cambridge: Cambridge University Press.

Boin, A., Ekengren, M., & Rhinard, M. (2014). *Making sense of sense-making: The EU's role in collecting, analysing, and disseminating information in times of crisis*. Stockholm: Swedish National Defence College.

Brady, H. (2012). *Saving Schengen. How to protect passport-free travel in Europe*. London: Centre for European Reform.

Ceuterick, L., & Weston, A. (2012). The EU operations centre permanent staff and the watchkeepers: Who they are and what they do. *Impetus. Bulletin of the EU Military Staff, 14*, 22–23.

Copernicus (2014). Copernicus emergency management service mapping. At http://emergency.copernicus.eu/mapping/#zoom=2&lat=12.11527&lon=58.22945&layers=0B000000T. Accessed 1 Feb 2015.

Cornelisse, G. (2014). What's Wrong With Schengen? Border Disputes and the Nature of Integration in the Area Without Internal Borders. *Common Market Law Review, 51*(3), 741–770.

Council of the EU (2001b, November 15). Report by the Secretary General/High Representative to the Council on intelligence cooperation, doc. 4546/1/01 REV1, Brussels.

Council of the EU (2003a, July 3). Suggestions for procedures for coherent, comprehensive EU crisis management, Annex to document 11127/03, Brussels.

Council of the EU (2007a). Annual report from the Council to the European Parliament on the main aspects and basic choices of the CFSP. At http://www.consilium.europa.eu/uedocs/cmsUpload/EN_PESC.pdf. Accessed 30 Sept 2012.

Council of the EU (2011d, June 20). Conflict prevention—Council conclusions, doc. 11820/11, Brussels.

Council of the EU (2012a, October 9). Council of the European Union, Annual report from the High Representative of the European Union for Foreign Affairs and Security Policy to the European Parliament, doc. 14605/1/12 REV 1, Brussels.

Council of the EU (2013, June 7). Finalisation of the CCA review process: The EU integrated political crisis response (IPCR) arrangements, doc. 10708/13 Brussels.

Council of the EU (2014a). The EU integrated political crisis response arrangements in brief. At http://www.consilium.europa.eu/workarea/downloadAsset.aspx?id=40802194085. Accessed 19 Dec 2014.

Council of the EU (2014b, July 1). Council Decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause. *Official Journal of the European Union, L 192.*

Council of the EU (2014d, July 23). Main aspects and basic choices of the CFSP (Part II, point E, paragraph 25 of the Interinstitutional Agreement of 2 December 2013)—2013—Annual report from the High Representative of the European Union for Foreign Affairs and Security Policy to the European Parliament, doc. 12094/14, Brussels.

Dent, C. (2013, July 12). Situational intelligence for effective decision making, critical communications. *Wired*. At http://www.wired.com/2013/07/situational-intelligence-for-effective-decision-making-critical-communications/. Accessed 17 Apr 2014.

DGA (2011). *DGA communication and information systems. 2010 Activity Report.* At http://bookshop.europa.eu/pl/dga-communication-and-information-systems-pbQCAL11001/;pgid=Iq1Ekni0.1lSR0OOK4MycO9B0000y58nN1Sb;sid=rv3kHr3MvnfkE-v1jLF6ud_pDD6YTh8P0q0=?CatalogCategoryID=luYKABst3IwAAAEjxJEY4e5L. Accessed 11 Jan 2012.

Di Stasio, J. (2015). *Situational intelligence as a risk management tool.* The situational intelligence blog. At http://situationalintelligence.net/situational-intelligence-as-a-risk-management-tool/. Accessed 21 May 2015.

Drent, M. (2011). The EU's comprehensive approach to security: A culture of co-ordination? *Studia Diplomatica*, *LXIV*(2), 3–18.

Duke, S. (2002). *The EU and crisis management: Development and prospects.* Maastricht: EIPA.

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

Duke, S. (2014). Intelligence and EU external relations: Operational to constitutive politics. In T. Blom & S. Vanhoonacker (Eds.), *The politics of information. The case of the European Union*. Basingstoke/New York: Palgrave Macmillan.

EEAS (2013a). EEAS privacy statement for the purpose of the processing operation upholding of EU Situation Room Contact Lists. At http://www.eeas.europa.eu/crisis-response/documents/2013/situation_room_data_protection_en.pdf. Accessed 20 July 2014.

EEAS (2014a). Crisis response and operational coordination factsheet. At http://eeas.europa.eu/delegations/un_geneva/documents/press_corner/focus/20130509_crisisresponse_facsheet.pdf. Accessed 14 Apr 2015.

EEAS (2014b). The EEAS crisis response & operational coordination department—What we do. At http://eeas.europa.eu/crisis-response/what-we-do/index_en.htm. Accessed 14 Apr 2015.

EEAS (2014c). Factsheet on crisis response and operational coordination department. At http://www.eeas.europa.eu/factsheets/docs/factsheets_europe_day_2014/factsheet_crisis-response_en.pdf. Accessed 14 Apr 2015.

Ekengren, M., & Groneleer, M. (2006). European Union crisis management: Challenges for research and practice. *International Journal of Emergency Management, 3*(1), 83–90.

European Commission (2010a, September 21). Communication from the commission on the global approach to transfers of passenger name record (PNR) data to third countries, doc. COM(2010) 492 final, Brussels.

European Council (1997, June 16). Amsterdam European Council, doc. SN00150/97, Brussels.

European Parliament (2009, December 1) Answer to the written question E-5998/09 from Martin Ehrenhauser, MEP, to the Council. Subject: Policy Planning and Early Warning Unit. At http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2009-5998&language=EN. Accessed 8 Mar 2013.

European Parliament (2012b, August 6). Answer given by High Representative/Vice-President Ashton on behalf of the Commission to the question for written answer E-006026/12 to the Commission (Vice-President/High Representative). Crisis Response and Operational Coordination Directorate (CROC)—Products and information. At http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2012-006026&language=EN. Accessed 8 Mar 2013.

European Union. (1997a). Declaration on the establishment of a policy planning and early warning unit. In *Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts.* Luxembourg: Office for Official Publications of the European Communities.

European Union. (1997b). Declaration relating to Western European Union. In *Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts.* Luxembourg: Office for Official Publications of the European Communities.

EUSC. (2015). *EU SatCen annual report 2014.* Luxembourg: Publications Office of the European Union.

Ferreira-Pereira, L. C., & Groom, A. J. R. (2010). 'Mutual solidarity' within the EU common foreign and security policy: What is the name of the game? *International Politics, 47*(6), 596–616.

Fishbein, W. H. (2011). Prospective sense-making: A realistic approach to 'foresight for prevention' in an age of complex threats. In Ch. de Franco & Ch. O. Meyer (Eds.), *Forecasting, warning, and responding to transnational risks.* Basingstoke/New York: Palgrave Macmillan.

Fishbein, W. & Treverton, G. (2004). *Making sense of transnational threats.* Occasional Papers, 3(1). Washington, DC: Sherman Kent Center for Intelligence Analysis.

Fuchs-Drapier, M. (2011). The European Union's solidarity clause in the event of a terrorist attack: Towards solidarity or maintaining sovereignty? *Journal of Contingencies and Crisis Management, 19*(4), 184–197.

Gebhard, C., & Norheim-Martinsen, P. M. (2011). Making sense of EU comprehensive security towards conceptual and analytical clarity. *European Security, 20*(2), 221–241.

Giegerich, B. (2010). Military and civilian capabilities for EU-led crisis-management operations. *Adelphi Papers, 50*(414), 41–58.

Gross, E. (2009). *The Europeanization of national foreign policy. Continuity and change in European crisis management.* Basingstoke/New York: Palgrave Macmillan.

Hatzigeorgopoulos, M. (2012). The EU's mutual assistance and solidarity clauses. *European Security Review, 61*, 1–10.

Hemmer, J., & Smits, R. (2011). *The early warning and conflict prevention capability of the council of the European Union. A mapping of the pre-lisbon period.* Brussels: IFP-EW/Clingendael.

High Representative (2013, December 11). Joint communication to the European Parliament and the Council. The EU's comprehensive approach to external conflict and crises, doc. JOIN(2013) 30 final, Brussels.

High Representative (2015, April 10). Joint staff working document. Taking forward the EU's Comprehensive Approach to external conflict and crises Action Plan 2015, doc. SWD(2015) 85 final, Brussels.

Horgby, A., & Rhinard, M. (2013). *The EU's internal security strategy: Living in the shadow of its past.* Occassional Paper no. 24. Stockholm: The Swedish Institute of International Affairs.

House of Lords (2003). *EU – Effective in a Crisis?* HL Paper 53. London: The Stationery Office.

House of Lords (2009). *Civil protection and crisis management in the European Union. Report with Evidence.* HL Paper 43. London: The Stationery Office.

Klein, G., Moon, B., & Hoffman, R. R. (2006). Making sense of sensemaking 1: Alternative perspectives. *IEEE Intelligent Systems, 21*(4), 70–73.

Koenig, N. (2014). Libya and the challenges of post-Lisbon crisis coordination. In D. Dialer, H. Neisser, & A. Opitz (Eds.), *The EU's external action service: Potentials for a one voice foreign policy.* Innsbruck: Innsbruck University Press.

Landaburu, E. (2008). A European perspective on crisis response. In A. Ricci (Ed.), *From early warning to early action? The debate on the enhancement of the EU's crisis response capability continues.* Luxembourg: Office for Official Publications of the European Communities.

Larsson, P. (2009). The Crisis Coordination Arrangements (CCA). In S. Olsson (Ed.), *Crisis management in the European Union. Cooperation in the face of emergencies.* Berlin/Heidelberg: Springer.

Larsson, P., Hagström Frisell, E., & Olsson, S. (2009). Understanding the crisis management system of the European Union. In S. Olsson (Ed.), *Crisis management in the European Union. Cooperation in the face of emergencies.* Berlin/Heidelberg: Springer.

Lennart, M. D., & Zandee, L. D. (2014). *The EU as a security provider.* Clingendael report. The Hague: Clingendael Institute. At http://www.clingendael.nl/sites/default/files/Report_EU_as_a_Security_Provider_december_2014.pdf. Accessed 1 Feb 2015.

Major, C., & Bail, M. (2011). Waiting for soft power: Why the EU struggles with civilian crisis management. In E. Gross et al. (Eds.), *Preventing conflict, managing crisis European and American perspectives.* Washington, DC: Center for Transatlantic Relations.

Manchin, J. (2014). Overview of crisis rooms. In P. Pawlak & A. Ricci (Eds.), *Crisis rooms: Towards a global network?* Paris: EU Institute for Security Studies.

Miozzo, A., & Missiroli, A. (2014). Foreword. In P. Pawlak & A. Ricci (Eds.), *Crisis rooms: Towards a global network?* Paris: EU Institute for Security Studies.

Mölling, Ch. (2008). Comprehensive approaches to international crisis management. *CSS Analyses in Security Policy, 3*(42). At http://www.css.ethz.ch/publications/pdfs/CSS-Analyses-42.pdf. Accessed 2 Feb 2013.

Moore, D. T. (2011). *Sensemaking. A structure for an intelligence revolution.* Washington, DC: National Defense Intelligence College.

Morsut, C. (2014). The EU's community mechanism for civil protection: Analysing its development. *Journal of Contingencies and Crisis Management, 22*(3), 143–149.

Mounier, G. (2009a). Civilian crisis management and the external dimension of JHA: Inceptive, functional and institutional similarities. *European Integration, 31*(1), 45–64.

Myrdal, S., & Rhinard, M. (2010). *The European Union's solidarity clause: Empty letter or effective tool?.* UI Occasional Paper. Stockholm: Swedish Institute of International Affairs.

Nimark, A., & Pawlak, P. (2014). Upgrading the Union's response to crises. In P. Pawlak & A. Ricci (Eds.), *Crisis rooms: Towards a global network?* Paris: EU Institute for Security Studies.

Olsson, S., & Larsson, P. (2009). The future of crisis management within the European Union. In S. Olsson (Ed.), *Crisis management in the European Union. Cooperation in the face of emergencies.* Berlin/Heidelberg: Springer.

Pawlak, P. (2014). Political and technical aspects of information sharing. In P. Pawlak & A. Ricci (Eds.), *Crisis rooms: Towards a global network?* Paris: EU Institute for Security Studies.

Peers, S. (2013). *The future of the Schengen system*. SIEPS Report No. 6. Stockholm: Swedish Institute for European Policy Studies.

Porfiriev, B. (2005). Managing crises in the EU: Some reflections of a non-EU scholar. *Journal of Contingencies and Crisis Management, 13*(4), 145–152.

Post, S. (2015). *Toward a whole-of-Europe approach. Organizing the European Union's and Member States' comprehensive crisis management*. Wiesbaden: Springer VS.

Rhinard, M., Ekengren, M., & Boin, A. (2006). The European Union's emerging protection space: Next steps for research and practice. *European Integration, 28*(5), 511–527.

Ricci, A. (2014). Definitions, controversies and challenges. In P. Pawlak & A. Ricci (Eds.), *Crisis rooms: Towards a global network?* Paris: EU Institute for Security Studies.

Shapcott, W. (2011). Do they listen? Communicating warnings: An intelligence practitioner's perspective. In Ch. de Franco & Ch. O. Meyer (Eds.), *Forecasting, warning, and responding to transnational risks*. Basingstoke/New York: Palgrave Macmillan.

Simonović, S. P. (2011). *Systems approach to management of disasters: Methods and applications*. Hoboken: Wiley.

Smith, M.E. (2013a). The European External Action Service and the security–development nexus: organizing for effectiveness or incoherence?. *Journal of European Public Policy, 20*(9), 1299–1315.

Stauffacher, D., et al. (2005). *Information and communication technology for peace. The role of ICT in preventing, responding to and recovering from conflict*. New York: The United Nations Information and Communication Technologies Task Force.

Tarîqa (2012).*Tarîqa 3.0 Installation Manual*. At http://joinup.ec.europa.eu/mailman/archives/tariqa-commits/2012-April/000010.html. Accessed 11 Mar 2015.

Tercovich, G. (2014). The EEAS crisis response system. *Journal of Contingencies and Crisis Management, 22*(3), 150–157.

Von Ondarza, N., & Parkes, R. (2010). *The EU in face of disaster: Implementing the Lisbon's treaty solidarity clause*. SWP comments no. 9. Berlin: German Institute for International and Security Affairs. At http://www.swp-berlin.org/fileadmin/contents/products/comments/2010C09_orz_pks_ks.pdf. Accessed 17 Mar 2013.

Zaiotti, R. (2013). The Italo-French row over Schengen, critical junctures, and the future of Europe's border regime. *Journal of Borderlands Studies, 28*(3), 337–354.

Zandén Kjellén, S. (2009). Rapid alerts for crises at the EU level. In S. Olsson (Ed.), *Crisis management in the European Union. Cooperation in the face of emergencies*. Berlin/Heidelberg: Springer.

CHAPTER 6

Socio-Cultural Intelligence in the EU

Diplomacy has always been connected to information and knowledge about other states, their political systems, economic resources, demographic features, cultural traits, etc. As foreign relations became global, more complex and interrelated, involving more actors belonging to different categories, state diplomacy needed increasingly to learn and understand different components of the world system, as they permeated state sovereignty and interfered in national interests and objectives.

The contemporary state has become dependent on reliable information sources. Decision-making processes require comprehensive information management and intelligence support to identify and evaluate the internal and foreign policy goals of the hosting state. Foreign diplomatic services obtain, collect and transmit information acquired in their receiving states (Herman 1996, p. 12). This information relates to various aspects of political, social, economic, cultural, religious, military, sporting or tourism activities.

Diplomatic posts are filled by both diplomats, or foreign-service officials, and intelligence officers, usually called spies. The former monitor the local environment, watching political, economic, social and cultural processes and developments, chart a course of action when necessary and provide reports describing or partially analysing the issues observed. They utilise open sources of information and intelligence products which are not subject to security clauses and basically remain unclassified. The latter, agents operating in embassies under deep cover, are tasked with acquiring

A. Gruszczak, *Intelligence Security in the European Union*,
DOI 10.1057/978-1-137-45512-3_6

information and data restricted or kept secret by local authorities or legal and private persons. This information and data—which can be raw material, a type of intelligence or a semi-intelligence product—is transferred back to the competent authorities of the sending country for further processing, collation or analysis.

Information provided by diplomats plays an increasingly important role in policy- and decision-making processes, especially in regard to security issues and 'hard' policy measures. The cognitive aspects of intelligence analysis cannot be separated from its cultural context (Davies 2004, pp. 496–9; Johnston 2005a, p. 6). In the present study, the cultural variable does not address the actual organisation and performance of an intelligence service or community. Nor does it focus on organisational culture, internal patterns of behaviour, sense-making in the organisation or the model of leadership. Most studies of national intelligence communities, especially US and British ones, have been dedicated to this issue. This book, however, seeks to accentuate the cultural context of strategic intelligence, the elements of culture and society in which the security environment is embedded, which is a plane of reference for situational awareness and risk assessment. In the twenty-first century, the principle 'know thy enemy' has been reoriented towards cultural studies, social research and religious analyses (Schneider and Post 2003). Good monitoring and surveillance of an area in which elevated risk and imminent threats are identified has become one of the core elements of modern intelligence tradecraft. Cultural awareness, reinforced by in-depth religious, ethnic and anthropological studies, has gained increasing relevance for national interests and international security regimes. Diplomacy has played a prominent role in intelligence security, providing insights into those security determinants that are located outside the traditional sphere of state influence. Knowledge of grass-roots cultural movements, powerful religious networks and indigenous sources of risk and menace has been increasingly relevant for intelligence communities at national and transnational levels.

Diplomacy has conventionally been involved in intelligence-type activities, given that policy making in this area needs robust, effective and firm intelligence support. An experienced US diplomat, John Brady Kiesling (2007, p. 239), stated that 'diplomacy and espionage live together in tense symbiosis'. That traditional view of diplomacy and intelligence has recently been rethought and conceptualised as socio-cultural intelligence (SOCINT). This concept takes into account numerous factors and determinants influencing contemporary foreign and security policies in the context of knowledge management, predictability and anticipation, situational awareness, and contingency planning.

Following the Lisbon treaty and the institutional reform of the Union, the orientation of the CFSP shifted towards enhanced diplomatic activities and more vigorous operational capabilities in the security field. The establishment of the EEAS was an important step on the way to genuine political actorness on the part of the EU. The incorporation of intelligence units (INTCEN, SitRoom, EUMS INT) into EEAS highlighted the growing importance of information management and analysis for the EU's decision-making mechanisms. The Treaty on European Union (European Union 2012, p. 35) stipulates in Article 35 that 'The diplomatic and consular missions of the Member States and the Union delegations in third countries and international conferences, and their representations to international organisations [...] shall step up cooperation by exchanging information and carrying out joint assessments.'

Notwithstanding these treaty provisions, there is already sufficient reason for cooperation and information exchange among diplomatic and consular services of Member States. The costs of independent information gathering are relatively high, even for large countries. This is a major stimulus for engagement in the collection of information and data (Dijkstra and Vanhoonacker 2011, p. 544). Despite the deficit of trust, Member States have quite often taken the opportunity to share information not only via bilateral channels, but increasingly through mechanisms and arrangements agreed at the EU level and implemented in the CFSP. More importantly, they have deliberately allowed the appropriate EU bodies to develop autonomous information-sharing capacities and welcomed analytical and intelligence deliverables resulting from information processing within the EU SOCINT system.

This chapter describes socio-cultural intelligence delivered by actors, institutions and agencies involved in EU external relations and common foreign policy. Knowledge of cultural, religious, normative, organisational and political factors seems to be a precondition of the broad scanning of the external environment that provides a more encompassing view of international security. The role of the High Representative (HR) and EEAS is central to the strategic assessment of the Union's external security. The effectiveness, credibility and relevance of the CFSP cannot be built without a strong networked mechanism of information gathering, processing and intelligence sharing among EU Member States, with EU institutions and agencies playing an active part. This requires the establishment of a socio-cultural intelligence hub integrating Member States' foreign ministries, diplomatic posts, EU institutions and agencies as well as the national intelligence services of the Member States.

Socio-Cultural Intelligence (SOCINT): Diplomacy in Support of Intelligence

Diplomacy is a state activity aimed at actively managing complex bilateral, regional and international relationships across a range of actors: the states, organisations, social and cultural movements, and ethnic communities that participate in international dialogue (Rana 2011, p. 4; Berridge 2011, pp. 9–14). As a result, contemporary diplomacy operates in a dense networked environment hosting a variety of subjects linked to local allies, national partners and overseas counterparts.

Diplomacy not only refers to partnership, good neighbourliness, and active and mutually beneficial cooperation, but also encompasses problems emerging at the supranational level—global challenges and universal dilemmas addressing the most existential questions underpinning national stability and international order. Diplomats and foreign-service officials no longer focus their activities exclusively and narrowly on national interests. They devote much of their attention to supranational and global issues and dilemmas because these constitute imminent and growing pressure on modern nation-states in terms of sovereignty, security, communication and governance. The proliferation of risks, threats and hazards has become a 'normal' feature of the modern world in the era of globalisation. The fact that sources of risk and origins of threats to national interests and values can be located far from state borders and outside the scope of the sovereign jurisdiction of a given state requires the role of traditional diplomacy to be redefined. This in turn is driving the shift towards the acquisition of information and management of knowledge gained through the analysis and interpretation of the social, political, cultural and economic environment.

Socio-cultural perspectives have gone hand in hand with state policies and decision-making processes since the dawn of human civilisation. Cultural knowledge, linguistic skills and organisational awareness were crucial for a comprehensive 'radiography' of 'the others', be they potential friends or bitter foes. Such a perspective was essential for strategic thinking, and determined the state's organisation, social attitudes, economic systems and defence capabilities. The external activities of state institutions, and the very primal forms of diplomacy, were focused on the ability to interact with foreign actors—statesmen, policy makers, local authorities and populations—in order to acquire thorough knowledge of their intentions, attitudes, outlooks and capabilities. From Sun Tzu, through Chanakya Kautilya, Alexander the Great, the Byzantine Emperor Maurice, Machiavelli, George Washington and Clausewitz to T.E. Lawrence, the principle 'know your enemy' was fundamental to strategic thinking, effective rule and *raison d'état*, or national interest (Keegan 2003, pp. 25–37). Thomas Edward Lawrence (2000, pp. 31–2), the British intelligence officer in the Middle East in the 1920s famously known as Lawrence of Arabia, concisely captured the essence of intelligence challenges in a new socio-cultural environment: 'A first difficulty of the Arab movement was to say who the Arabs were. […] The origin of these peoples was an academic question; but for the understanding of their revolt their present social and political differences were important, and could only be grasped by looking at their geography.'

Apart from definitional problems beyond the scope of the present study, strategic culture can be understood as a set of socially transmitted norms, patterns of thought and modes of action derived from historical experience, geopolitical position, economic development, political culture and military organisation, related to ensuring the survival and growth of a particular political community (the nation, the state, international organisation) through deliberately devised ends and means for achieving security objectives (Gray 1984, pp. 26–33; 1999a, pp. 49–69; Booth 1979, 2005, pp. 25–6; Johnston 1995, pp. 33–6; Mahnken 2006, pp. 4–9; Johnson et al. 2009, pp. 3–14; Lantis 2009, pp. 33–52). As a domain of collective actors following patterns of cooperation and rivalry, security can be said to be predetermined by functional and behavioural incentives embedded in culture. This seems obvious with regard to national security cultures, where security is subject mostly to national sovereign interests as well as individual actions and collective policies based on shared beliefs and a sense of community. It is more questionable if one examines an international organisation built on specific sources of identity, a common pool of values, norms and attitudes as well as different traditions of 'doing security'.

Social, cultural, psychological and anthropological traits have also been considered from a more specific angle, determined by questions of cultural identity, national security, strategic thought and 'ways of warfare'. The concept of strategic culture was introduced in the 1970s and has developed into an influential and negotiable analytical framework for the analysis of cultural impact on policy choices and outcomes (Johnston 1995; Gray 1999b, Chap. 5; Sondhaus 2006; Jones 2012b, pp. 297–9). Ken Booth, one of the most influential proponents of the concept of strategic culture, argued that 'understanding strategic culture is a fundamental part of "know thine enemy and know thy self", emphasising such factors as beliefs, assumptions and modes of behavior which shape the security environment'. He also asserted that strategic culture should be underpinned by 'strategic anthropology' (Booth 2005, p. 26; comp. Gray 2013), given that the notion of the self is at the heart of security and politics (Booth 1994).

Lessons learned by politicians, the military and scholars when managing, resolving or studying conflicts in the Balkans, the Middle East, the Horn of Africa, the Persian Gulf, North Africa and—last but not least—the AfPak area evidence the growing relevance of cultural and religious determinants as well as social and psychological factors. Given that prediction, prevention and early warning, as essential parts of national security strategies and policies, were overwhelmingly dominated by advanced electronic systems using state-of-the-art surveillance technologies, the intensity of the violent cultural backlash, so stark in asymmetric conflicts, brought shock and awe to the Western states and societies that were parties to those conflicts. Routine collection of intelligence from traditional sources came back into favour, highlighting the relevance of socio-cultural factors for appropriate situational awareness, risk assessment and threat profiling.

Socio-cultural intelligence seeks, according to Sorentino (2011), 'to utilize this enhanced capability to understand the *why* factor as it applies to their behavior and *how* that behavior is being driven by their mindsets, perceptions, beliefs, customs, ideologies and religious influences'. Patton (2010, p. 14) argues that 'Incorporating the sociocultural information provides situational understanding and predictability in anticipating overpressure or second and third order of effects possibilities'.

The scope of socio-cultural intelligence is very large, encompassing such divergent elements of information and knowledge as:

1. religious, political, and ethnic affiliations,
2. customs and habits,
3. mechanisms of political activation and recruitment,
4. important dates,

5. communication and transportation infrastructure,
6. health service and medical assistance,
7. means and methods of communicating to the public (Patton 2010, p. 23).

According to social network theory, certain features of society or its cultural formation can be identified and understood through context analysis in a given networked environment layered with topographical maps. Socio-cultural intelligence emphasises the cognitive, behavioural and volitional aspects of individual attitudes and actions. It puts individual behaviour in the context of social networks and, by applying cross-disciplinary studies, seeks to identify specific features influencing group behaviour or structural characteristics of institutions and organisations.

The Institutional Dimension of Intelligence Cooperation for the CFSP

With the entry into force of the Lisbon treaty, existing elements of intelligence support for the CFSP were gradually incorporated into the new structures of EU external relations, foreign and security policies. The High Representative, now officially responsible for EU foreign affairs and security policy, was granted a plethora of units and bodies making up an expanded and diversified institutional network denominated as EEAS. The European External Action Service was formally established as a diplomatic corps, taking over from the former DG RELEX (Directorate-General for External Relations, belonging in the European Commission) yet also incorporating intergovernmental units or working groups dedicated to security issues. New organisational elements emerged aimed at enhancing the security dimension of the external activities of the EU as an international actor.

The Council (2007b, p. 4), in accordance with the conclusions adopted in November 2007, put stronger emphasis on the coherence and consistency of external actions, which should be achieved by improving strategic planning through systematic situational assessments and conflict analyses.

EC delegations were called upon to enhance crisis-response capacities, monitor deteriorating situations, alert the Commission and provide all available and relevant information via a crisis correspondents' network. It was also agreed that regional crisis-response planners would be deployed, with the task of monitoring the situation in a crisis area (Council of the

EU 2008a, pp. 5–6). Initially the planners were dispatched to seven EC delegations.

EEAS consolidated hitherto dispersed components of security and defence policy and also facilitated the reinforcement of EU diplomatic structures, especially EU delegations in third countries and at international organisations. It was a hybrid combination of institutional segments in charge of diplomacy, external relations and regional development, with organisational components responsible for civil and military aspects of security and defence. The HR/VP played the role of coordination hub, linking the foreign policy field with the security and defence area and, assisted by the Political Affairs Department, providing practical and systemic intelligence support for foreign affairs and diplomatic activities falling within the scope of EEAS's competences. The HR/VP is also supported by the Policy Planning and Early Warning Unit (PPEWU) created under the Amsterdam treaty. PPEWU officials were recruited from the Member States and the General Secretariat of the Council and the Commission (Soetendorp 1999, p. 73; Salmon and Shepherd 2003, pp. 88–9; Stewart 2006, pp. 116–7); their role, in close collaboration with the CFSP unit, is to advise the presidency and the High Representative on the implementation of 'policies and priorities defined by the European Council and the Council of Ministers', and be able to collect and analyse all relevant information, including confidential data gathered by EU embassies and chancelleries.

The HR/VP's position as liaison between the CSDP and the common foreign policy was further highlighted by certain specific arrangements concerning security policy and CSDP structures, especially those concerned with preparing, conducting and managing military missions and tasks. Although the EU Military Staff along with the Crisis Management Planning Directorate and the Civilian Planning and Conduct Capability were framed within EEAS, they nonetheless kept their intergovernmental character and *modus operandi*, having belonged before the Lisbon reform in the General Secretariat of the Council. By the same token, INTCEN was placed under the direct authority and responsibility of the High Representative. One of its main tasks was to provide support for the Council during the preparation and conduct of crisis-management operations. In the area of CFSP, the main objectives for INTCEN included:

- to contribute to the early warning work of the Council and the High Representative;

- to undertake situation monitoring and assessment;
- to provide specialised back-up to crisis task forces requiring intelligence and situational awareness for their field activities;
- to provide support for the Council and the High Representative during the preparation and conduct of crisis management operations, fact-finding missions, and the visits of EU Special Envoys under a CFSP mandate (House of Lords 2003, p. 25; European Parliament 2009).

Following the post-Lisbon reform, INTCEN took part in the development of the EU's common foreign policy, focusing on crisis-detection and early warning elements. It contributed, along with EUMS and DG RELEX, to a confidential document called the Watchlist, which listed states the EU ought to monitor closely in the context of possible crises or proliferating threats (see Chap.5). INTCEN has also become involved in the consular affairs of EU Member States. It monitors, on a daily basis, the number of EU citizens in each country of interest, offering central information on specific consular issues. This is done through Consular Online (CoOL), a Web-based information-exchange system granting access to its resources to all authorised stakeholders: Member States, EU institutions and agencies or EU delegations (Schrumpf and Stam 2012, p. 20).

INTCEN's analytical products mostly depend on Member States' intelligence and security services. These are expected to provide the centre with information or other kind of analytical input on request, except for raw intelligence and operational information (Jones 2012a, p. 3). The agency may also access selected information originating in Member States' diplomatic cables transmitted via the secure diplomatic network COREU. In fact, the real value of national contributions to INTCEN's performance depends greatly on the readiness to cooperate, capacity to share and willingness to deliver on the part of EU members. Given the constant deficit of valuable information and data of national origins, INTCEN is forced to rely on dispersed EU sources, such as EU delegations and offices around the globe, CSDP staff seconded to participate in external missions and operations, and fact-finding teams and visits.

Fact-finding missions are forms of socio-cultural intelligence activity that enable EU representatives to directly observe security challenges or dilemmas on the spot and to build situational awareness and risk assessment on the basis of original information and raw data. They are of relatively short duration (not exceeding a week) and aim to reduce the information and knowledge deficit about the crisis area. The composition of a fact-finding team is flexible. An intelligence officer seconded by INTCEN usually is included in the team (Dijkstra 2013, p. 82).

The European Union's Special Representatives (EUSRs) and Special Envoys are other important contributors to the EU socio-cultural intelligence apparatus (Hynek 2011, pp. 88–9). In spite of the Lisbon treaty reform and the establishment of EEAS, the Special Representatives were not incorporated into this service and are not part of the EEAS hierarchy (Tolksdorf 2012, p. 1). The practice of appointing Special Envoys for constructive and effective engagement in political-diplomatic processes relevant for EU foreign and security policies dates back to the mid-1990s. The first ever Special Envoys were deployed in 1996 in the Great Lakes region of Africa and for the Middle East peace process. With the establishment of the High Representative for the CFSP, the Treaty of Amsterdam also provided for Special Representatives to be appointed by the Council, which would provide them with a mandate in relation to particular policy issues (European Union 1997a).

The appointment of experienced diplomats, politicians or government officials from Member States as EU emissaries with specific tasks overseas can be seen as evidence of the growing involvement of the EU globally in conflict prevention, crisis management, post-conflict stabilisation and peace maintenance. The Council's decisions clearly reflected the EU's external relations priorities as well as CFSP guidelines. EUSRs were seconded to countries, regions or organisations particularly relevant to CFSP security concerns and to the EU's legitimacy as peacemaker and stabiliser in conflict-prone areas and zones of protracted crises. The deployment map of the Special Representatives and Special Envoys basically overlapped that of EU civilian and military missions. It encompassed such regions and countries as the Balkans (Bosnia and Herzegovina, the former Yugoslav Republic of Macedonia, Kosovo), Moldova, the South Caucasus, Central Asia, Afghanistan, the Southern Mediterranean region, the Sahel, the African Great Lakes, the Horn of Africa and Sudan. EUSRs were also appointed to carry out the tasks defined in the Middle East peace process and in the Stability Pact for South-Eastern Europe as well as to strengthen human rights and democracy in EU external actions.

The EUSRs report to the High Representative and the Political and Security Committee. The PSC provides strategic direction and exercises political control. The EUSRs are expected to ensure the timely reporting and analysis of relevant information and developments for the High

Representative and other CFSP units, especially in cases of rapidly unfolding crises. They facilitate the pooling of conflict-management resources and help to coordinate the action of all EU actors involved (Council of the EU 2007a, pp. 93–4). This input is significant for policy adjustment and decision making at EU institution level. As Grevi (2007a, p. 38) points out, Special Representatives 'perform as an interface to streamline the two-way flow of information between the field and headquarters', fuelling policy initiatives at EU level. Good, fast and reliable information flow from the EUSRs to Brussels makes a significant contribution to the effectiveness of EU diplomacy, especially in emergency situations or in the face of rapidly unfolding local or regional crises (Grevi 2007b, pp. 1–5). EU representatives and envoys acquire information and data on the ground, and supply them for processing to field-based team members who prepare analytical reports transmitted directly to headquarters in Brussels.

It can be seen from this description of the units and bodies providing intelligence support for CFSP missions and crisis management that the organisational culture of EEAS fails to achieve clarity, functionality and effectiveness as a new institutional setting for foreign and security policies of the EU. The strategic uncertainties and complexities surrounding the EU as a regional and global security actor demands a constantly increasing inflow of information and data for both prevention and policy planning purposes, which proves feasible only if it is professionally and completely processed and turned into intelligence products. Levels of information management and data sharing are still inadequate for compiling a comprehensive socio-cultural intelligence complex to contribute decisively to the decision-making processes and operational activities of EU institutions and forces.

Communication and Intelligence Sharing in the CFSP

Strategic information, sensitive data and confidential communication require secure transmission channels. The extensive circulation of information within CFSP structures poses certain challenges of coordination, control and responsibility. Although these challenges had been identified as early as the 1970s, it was only after the emergence of the genuine CFSP within the EU that technical and organisational solutions emerged. Several secure communication networks were built to facilitate information exchange between the main stakeholders, national and supranational, as well as to enhance the decision-making capabilities of EU institutions in the field of foreign and security policies.

The first and most important of these networks is COREU. Together with ESDPNet it has been the predominant player in guaranteeing a proper communication mechanism for the use of EU institutions, agencies and bodies, and relevant authorities of the Member States.

COREU is an acronym for Correspondence Européenne. It is an encrypted communication network transmitting messages referring to foreign and security affairs and regulating secure information flows in the CFSP area. The COREU network links European correspondents in the foreign ministries of EU Member States with their respective permanent representatives in Brussels and the EU institutions involved in the CFSP: the European Commission and the General Secretariat of the Council. Most importantly, COREU is closely connected with EEAS. This 'functionally autonomous body of the Union under the authority of the High Representative' was constituted by the Lisbon treaty to 'assist the President of the European Council, the President of the Commission, and the Commission in the exercise of their respective functions in the area of external relations' (Council of the EU 2010b, p. 30). According to Bicchi and Carta (2012, p. 472), EEAS is 'a pivotal actor in the circulation of information' via COREU.

COREU was established in 1973 under the Danish presidency of the then Council of Ministers. Politically it stemmed from the Copenhagen Report of July 1973 (Nuttall 1992, p. 23; Smith 2004b, pp. 94–5), which praised the European Political Cooperation (EPC) as a framework for closer foreign policy consultations between EC Member States (Smith 2004a, pp. 104–6; Sjursen 2006, pp. 96–7; Jones 2007, pp. 78–9). The foreign ministers agreed to set up a group of 'European correspondents' in the foreign ministries of every Member State and connect them to a communication system based on the secure telex network. This was an innovative solution to existing communication practices which were based on sporadic bilateral exchanges. The COREU network enabled the simultaneous horizontal transmission of information and communication related to EPC issues to the foreign offices of all EC Member States. It also prompted vertical information flows within national ministries for foreign affairs by granting officials at all levels access to COREU outputs via in-house channels, helping them to determine their national position on a given matter of concern and forward it for further deliberation within the EPC. COREU was administered by the Dutch Ministry for Foreign Affairs and was regarded as 'the only permanent, collectively financed manifestation of European foreign policy until 1986' (Smith 2004b, p. 94). The system was quickly accepted by officials in foreign ministries as a useful tool with which to communicate national positions and standpoints to the remaining Member States and eventually to consult or debate on particular issues within a matter of hours. As a result, the number of messages telexed via COREU quickly reached several thousand per year and in 1991, on the eve of the Maastricht Treaty, it exceeded 10,000. The COREU network underwent technical developments, modifications and updates to enable the exchange or transmission of more sensitive information touching on military and security issues (Smith 2004b, p. 102).

Member States play the fundamental role in the COREU workflow, feeding the system with cables, briefs, drafts, estimates and reports. Their embassies in Brussels are also connected to the communication system. However, Permanent Representatives to the EU are passive recipients (Bicchi and Carta 2012, p. 469). They cannot react directly to the messages or give feedback to the original source, though they can provide insights to their ministries and thereby contribute to multilateral exchange.

COREU is meant to be a useful communication tool for the presidency in the Council. The Member State presiding over the Council is expected to increase the amount of correspondence both before the start of a presidency and over the course of the subsequent work of the Council (Bicchi 2011, pp. 1121–2). Given the responsibility in the field of CFSP incumbent upon the Member State holding the presidency, effective representation of the EU in its external relations, as well as proper management of security-related issues, require a well functioning system of information flow, data exchange and the sharing of pre-processed knowledge or analytical products. Interestingly, guidelines for the diplomatic representation of the presidency by another Member State in third countries in the field of CFSP, adopted by the Council in 2006, contain certain non-binding rules concerning the communication system, information exchange and the use of COREU for decision-making and consultation purposes (Council of the EU 2007c, p. 14).

It is not only multilateral arrangements made by national actors but also principles of regional integration defined in EU law and treaty provisions that form a single security community. The supranational dimension of this cooperation is reflected in the institutional context, with the EEAS acting through its own European Correspondent,[1] and the Council, but not the European Parliament, delivering substantial inputs and technical and organisational support.

EEAS's classified information management system is built on several platforms transferred from the General Secretariat of the Council (GSC) and from the Commission, although at the end of 2013 the management of these systems was still in transition. The most important and best developed of these is CORTESY, which stands for COREU Terminal Equipment System (Duke 2006, p. 612), installed in 1996. CORTESY plays an auxiliary role to COREU with respect to the official exchange of classified diplomatic information; COREU messages are channelled through the CORTESY system and dispatched to authorised customers, Member States' foreign ministries and Permanent Representations to the EU, EEAS, GSC and INTCEN.

EU delegations in third countries receive COREU messages on a need-to-know basis. The classified information management system guarantees secure transmission of files from EEAS headquarters to the delegations. The encrypted communication with the associated countries is maintained via the ACN network. It enables official document exchange (LIMITE and RESTREINT UE) between the Council, the ministries of foreign affairs their diplomatic missions in Brussels.[2] A similar network, ACD, dedicated to the acceding countries, has also been developed (DGA 2011, p. 32), but was not in yet in operation by the end of 2015.

ESDPNet is a platform used to exchange classified information in the CFSP and CSDP domains. It was originally established as a secure communication system of the Western European Union, but on the transfer of the organisation's capabilities and functions to the EU, the network was renamed ESDPNet and merged with CORTESY. It provides a high-security link between EU Military Staff and operational headquarters.

In early 2002, with preparations for the first CSDP missions in the Balkans, and in the context of an increased level of risk post-9/11, the GSC proposed the SESAME project to replace ESDPNet as a secure communication platform for consultation, decision-making processes and crisis-management policy/planning activities in the realms of CFSP and CSDP (DGA 2011, p. 32). SESAME is based on a single integrated system comprising two main layers of classification. Information uploaded to the system is identified according to the level of its security clearance and redirected to an appropriate transmission channel. The first channel handles information up to RESTREINT UE; the second deals with information classified CONFIDENTIEL UE and SECRET UE. As noted in Chap. 4, the system is not yet operational.

Partly in response to deadlock in the SESAME project, in 2010 EUMS initiated a project called Military Intelligence System Support. This was aimed at providing a secure connectivity system for the exchange of classified information among the CSDP stakeholders. With the establishment of EEAS, the project was defined within the new institutional framework, although it was still at an embryonic stage. In 2012 it was renamed 'EEAS-wide Civ/Mil Intelligence System Support'. It kept 'project status', with no further details made available to the public (European Parliament 2012c).

In July 2013, an EEAS review report by the High Representative stated that the service was working on the integration, upgrading and modification of the existing platforms to ensure greater use of joint reports and sharing of information between EU delegations and embassies of Member States in third countries, including non-resident EU ambassadors (EEAS 2013c, p. 17). By the end of 2015, however, no changes had been made in the IT secure systems and CORTESY/ESDPNet remained the principal secure communication system for the CFSP.

Socio-Cultural Intelligence in Action: The Case of North Africa

The Arab Spring provides an interesting example of crisis-response mechanisms triggered outside the Union but engaging CFSP tools. It was the first major crisis after the launch of the fully fledged post-Lisbon CFSP in its new legal and institutional framework. The crisis occurred in close proximity to the territory of EU Member States and concerned countries developing various forms of cooperation and partnership with the EU. Moreover, the dynamic of this regional crisis demanded a resolute and appropriate response on the part of EU diplomacy in order to prevent escalation of the conflicts and possible negative consequences for the EU.

The EU's reaction, though rapid, was mixed, and focused both on consular protection of EU citizens and opportunities for gaining a decisive influence over developments in North Africa, particularly in Egypt and Libya. The need for a good situational assessment of the dynamics of popular uprisings and anti-regime forces prompted EC delegations in that part of the world to increase their monitoring and assessment of the ongoing events. However, certain weaknesses and limitations in the scope and quality of EU diplomatic representation have been identified by decision makers, experts and scholars. Given the gravity of the situation in North Africa, the multitude of risks and dangers identified in that area (massive migration, Islamic fundamentalism, political radicalism), and the evident weaknesses of EU assets, the question of strategic awareness and a comprehensive assessment of the security environment in North Africa was highly problematic.

Babaud and Mirimanova, who proposed a synthetic view of the EC framework and organisational structures related to early warning, observe: 'EC Delegations in third countries vary in their activity and capacity with regards to gathering and analysing information on potential conflicts and emerging or ongoing crises. Some Delegations are staffed with political officers whose role is to monitor political and security situations. Some Delegations in countries suffering from protracted conflicts also have special staff that deal with conflict, including issuing early-warning signals. Other Delegations are not equipped with this specific expertise and therefore do not gather conflict early-warning information in any systematic way' (Babaud and Mirimanova 2011, p. 11).

The problem with North Africa was the deficit of reliable, accurate and up-to-date information originating from local sources. It was extremely difficult to build situational awareness and shape a rapid and proper reaction to the dynamics of the conflicts. An immediate and comprehensive solution was needed. The second problem lay in unequal EU diplomatic representation, starting with the absence of an EC delegation and several national embassies in Libya, a country with a large number of residents from EU Member States.

The deficit of situational awareness prompted EU crisis-response units to launch special missions and activate available sources of information. In June 2011 the Managing Director for EU crisis response and operational coordination revealed to the press that EEAS had helped the League of Arab States build a situation room to reinforce the League's analytical capabilities and situational awareness as well as to enhance its ability to tackle future crises effectively (Rettman 2012; Abu Ghazaleh 2014, p. 54). The 'Arab SitRoom' was located in Cairo, close to the Arab League chief's office. It was equipped with 2 million euros' worth of high-tech electronic devices and communication systems driven by dedicated software. According to the European Commission, the Situation Room started in 2008 as a joint project of the EU and the UN Development Programme's regional office in Cairo, which provided technical assistance. It aimed at 'creating a crisis response capability, that is effective early warning by using open source information' and was coordinated by the EU Delegation in Egypt (European Parliament 2012d). During the Arab Spring, work on this project was considerably accelerated, and was completed in June 2011. The 'Arab SitRoom' was designed to actively facilitate a more direct, frequent and informal sharing of views, including the exchange of non-classified political and operational conclusions, among representatives of the EU, the UN and the Arab League. In particular, the European Union and the United Nations could share their best practices on conflict prevention, peace building and crisis response with the Arab States. Moreover, the Commission evaluated the Arab SitRoom project as 'a sound investment for the EU', which could improve the situational awareness capacity of and consolidate EU influences in North Africa (European Parliament 2012d).

Another example of socio-cultural intelligence activities in North Africa is the Libyan turmoil, civil war and military intervention. With the outbreak of the anti-Gaddafi uprising, crisis-management structures in the EU were understaffed and lacked expertise (Koenig 2014, p. 169). Meanwhile, several thousand citizens of EU Member States residing in Libya were anticipating EU protection and assistance in evacuating this war-torn country. EEAS sent a fact-finding mission to Libya and demanded all possible intelligence support from the relevant EU bodies. The Joint Situation Centre was involved in EEAS fact-finding missions in Libya, supposedly to Tripoli and Benghazi, in March and April 2011. According to Ilkka Salmi, head of INTCEN, the tasks assigned to INTCEN officials were more supportive than operational (Rettman 2011). The agency sent a technical person to secure communication with Brussels (Clerix 2014). The EU also activated the Crisis Platform, which convened frequently during the escalation of the Libyan turmoil. Likewise, the Consular Online (CoOL) website was used to facilitate consular cooperation during the evacuation of EU citizens. Boin et al. (2014, p. 31) point out that 'the website was used as intended, to share information and support coordination between its users during a crisis'. Certainly, neither fact-finding missions nor information exchange via CoOL were intelligence driven. They were, however, geared to gathering and exchanging information with local sources. This information was later used for further assessment and analysis and incorporated into EEAS intelligence production.

Conclusions

The tremendous expansion of global communication networks engaging hundreds of millions of individuals all over the world has led to recent progress in intelligence studies. Social media have enhanced the effects of the 'digital tsunami' and created both challenges and opportunities for state authorities responsible for security and public order. Cultural, religious and societal factors have become increasingly important for situational awareness, risk assessment and policy planning. For now, there is no doubt that socio-cultural perspectives could be used more widely in intelligence analysis.

The European Union, as a 'soft' actor on the international stage, has no single intelligence agency and maintains a multi-centric network of intelligence units and bodies with limited opportunities for data exchange and intelligence sharing. The firm stance of some Member States on intelligence cooperation through EU bodies shifts the burden of responsibility for the preparation and implementation of emergency measures onto EU structures.

The integration of EUMS with EEAS redefined the objectives and tasks of the Military Staff towards a greater involvement in security and defence policy areas, but also stronger support for diplomatic and civilian missions abroad. The external dimension of EU integration policies meant strengthening the diplomatic leverage of the EU and ensuring proper coordination between EU diplomatic actions and military-led activities in the areas of conflict prevention and crisis management, as well as post-conflict rebuilding and stabilisation.

The European Union has developed and constantly improved communication and information management systems. These systems and networks, especially COREU, CORTESY and ESDPNet, require constant modernisation and development, as well as better adjustment to the practical diplomatic activities within the CFSP. COREU, for example, has developed its transmission capacity but still seeks to optimise the management of information delivered to EEAS. COREU enables large-scale information flow, yet it is less efficient when specific information is needed in Brussels or when targeted knowledge should be rapidly exchanged between EEAS and EU delegations. In extraordinary circumstances COREU is in fact a useless tool and much strategic communication is conducted outside this network.[3]

The expanding diplomatic network of EU delegations, representations, missions and task forces abroad enables a large volume of data and information to be acquired, processed and used in EU-led processes of early warning, conflict prevention and crisis management. Socio-cultural intelligence seems to be a good solution to the structural and organisational problems of EU intelligence cooperation in the CFSP area, since it enables the expanded diplomatic network established by the Commission and EEAS in third countries and organisations to be linked to dedicated intelligence units located within EEAS. The Arab Spring provided interesting examples of crisis-response mechanisms triggered outside the EU but engaging CFSP tools.

The European Union has proved that it has the capacity to use socio-cultural intelligence. Diplomatic missions and delegations, Special Representatives and Envoys dispatched throughout the world are able to gather publicly available information from various sources. Some scholars claim that EU representatives 'through their local contacts may occasionally obtain confidential information. They also may have detailed knowledge of specific issues and can place developments in the proper context for decision makers' (Walsh 2009, p. 15). This does not mean that EU officials practise systematic collection or analysis of intelligence. They simply benefit from available local diplomatic, social and political sources and make the acquired information available to EEAS intelligence units.

Notes

1. The Commission before the establishment of EEAS had its European correspondent located in DG RELEX.
2. These countries were Macedonia, Serbia, Montenegro, and Turkey, as of 1 January 2014.
3. Anonymous EEAS official, interview, October 2013.

Bibliography

Abu Ghazaleh, H. (2014). Crisis rooms in the Arab word. In P. Pawlak & A. Ricci (Eds.), *Crisis rooms: Towards a global network?* Paris: EU Institute for Security Studies.

Babaud, S., & Mirimanova, N. (2011). *The European Commission early-warning architecture and crisis-response capacity*. Brussels: IFP-EW/International Alert.

Berridge, G. R. (2011). *The counter-revolution in diplomacy and other essays.* Basingstoke/New York: Palgrave Macmillan.

Bicchi, F. (2011). The EU as a community of practice: Foreign policy communications in the COREU network. *Journal of European Public Policy, 18*(8), 1115–1132.

Bicchi, F., & Carta, C. (2012). The COREU network and the circulation of information within EU Foreign policy. *Journal of European Integration, 34*(5), 465–484.

Boin, A., Ekengren, M., & Rhinard, M. (2014). *Making sense of sense-making: The EU's role in collecting, analysing, and disseminating information in times of crisis*. Stockholm: Swedish National Defence College.

Booth, K. (1979). *Strategy and ethnocentrism*. New York: Holmes and Meier.

Booth, K. (1994). *Security and self. Reflections of a fallen realist*. YCISS Occasional Paper No. 26, Toronto: York Centre for International and Security Studies.

Booth, K. (2005). Strategic culture: Validity and validation. *Oxford Journal on Global Governance, 2*(1), 25–28.

Clerix, K. (2014). Ilkka Salmi, the EU's spymaster. *Mondiaal Nieuws*, 4 March. At http://www.mo.be/en/interview/ilkka-salmi-eu-s-007. Accessed 10 June 2014.

Council of the EU (2007a). Annual report from the Council to the European Parliament on the main aspects and basic choices of the CFSP. At http://www.consilium.europa.eu/uedocs/cmsUpload/EN_PESC.pdf. Accessed 30 Sept 2012.

Council of the EU (2007b, November 20). Conclusions of the council and the representatives of the Governments of the Member States Meeting Within the Council on security and development, doc. 15097/07, Brussels.

Council of the EU (2007c, November 6). "CFSP guide"—Compilation of relevant texts, doc. 14703/07, Brussels.

Council of the EU (2008a, June 17). Annual report on EU activities in the framework of conflict prevention, including implementation of the EU programme for the prevention of violent conflicts, doc. 10601/08 Brussels.

Council of the EU (2010b, August 3). Council decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service. *Official Journal of the European Union, L 201*.

Davies, P. H. J. (2004). Intelligence culture and intelligence failure in Britain and the United States. *Cambridge Review of International Affairs, 17*(3), 495–520.

DGA (2011). *DGA communication and information systems. 2010 Activity Report*. At http://bookshop.europa.eu/pl/dga-communication-and-information-systems-pbQCAL11001/;pgid=Iq1Ekni0.1lSR0OOK4MycO9B0000y58nN1Sb;sid=rv3kHr3MvnfkE-v1jLF6ud_pDD6YTh8P0q0=?CatalogCategoryID=luYKABst3IwAAAEjxJEY4e5L. Accessed 11 Jan 2012.

Dijkstra, H. (2013). *Policy-making in EU security and defense. An institutional perspective*. Basingstoke/New York: Palgrave Macmillan.

Dijkstra, H., & Vanhoonacker, S. (2011). The changing politics of information in European foreign policy. *Journal of European Integration, 33*(5), 541–558.

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

EEAS (2013c). EEAS review. At http://eeas.europa.eu/library/publications/2013/3/2013_eeas_review_en.pdf. Accessed 7 May 2014.

European Parliament (2009, December 1) Answer to the written question E-5998/09 from Martin Ehrenhauser, MEP, to the Council. Subject: Policy Planning and Early Warning Unit. At http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2009-5998&language=EN. Accessed 8 Mar 2013.

European Parliament (2012c, November 30). Answer to the written question E-006023/12 from Martin Ehrenhauser, MEP, to the Commission (Vice-President/High Representative). Subject: Military Intelligence System Support (MISS), 19 June. *Official Journal of the European Union, C 286 E.*

European Parliament (2012d, August 14). Answer to the written question E-006364/12 from Lucas Hartong, MEP, and Auke Zijlstra, MEP, to the Commission. Subject: Building of Arab League 'situation room' in Cairo. At http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2012-006364&language=EN. Accessed 8 Mar 2013.

European Union (2012). Treaty on European Union (consolidated version). *Official Journal of the European Union*, C 326, 26 October.

Gray, C. S. (1984). Comparative strategic cultures. *Parameters, 14*(4), 26–33.

Gray, C. S. (1999a). Strategic culture as context: The first generation of theory strikes back. *Review of International Studies, 25*(1), 49–69.

Gray, C. S. (1999b). *Modern strategy*. Oxford: Oxford University Press.

Gray, C. S. (2013). The strategic anthropologist. *International Affairs, 89*(5), 1285–1295.

Grevi, G. (2007a). *Pioneering foreign policy. The EU special representatives*. Chaillot Paper No. 106. Paris: European Union Institute of Security Studies.

Grevi, G. (2007b). Making EU foreign policy: The role of the EU special representatives. *CFSP Forum, 5*(5), 1–5.

Herman, M. (1996). *Intelligence power in peace and war*. Cambridge: Cambridge University Press.

House of Lords (2003). *EU – Effective in a Crisis?* HL Paper 53. London: The Stationery Office.

Hynek, N. (2011). EU crisis management after the Lisbon Treaty: Civil–military coordination and the future of the EU OHQ. *European Security, 20*(1), 81–102.

Johnson, J. L., Kartchner, K. M., & Larsen, J. A. (2009). Introduction. In J. L. Johnson, K. M. Kartchner, & J. A. Larsen (Eds.), *Strategic culture and weapons of mass destruction: Culturally based insights into comparative national security policymaking*. London/New York: Palgrave Macmillan.

Johnston, A. I. (1995). Thinking about strategic culture. *International Security, 19*(4), 32–64.

Jones, S. G. (2007). *The rise of European security cooperation*. Cambridge: Cambridge University Press.

Jones, Ch. (2012a). Secrecy reigns at the EU's Intelligence Analysis Centre. *Statewatch*, 22(4), 3–6.

Jones, F.L. (2012b). Strategic Thinking and Culture: A Framework for Analysis. In J.B. Bartholomees, Jr. (Ed.), *U.S. Army War College Guide to National Security Issues. Volume II: National Security Policy And Strategy,* 5th ed. Carlisle: U.S. Army War College.

Keegan, J. (2003). *Intelligence in war. Knowledge of the enemy from Napoleon to al-Qaeda*. London: Hutchinson.

Kiesling, J. B. (2007). *Diplomacy lessons: Realism for an unloved superpower*. Washington, DC: Potomac Books.

Koenig, N. (2014). Libya and the challenges of post-Lisbon crisis coordination. In D. Dialer, H. Neisser, & A. Opitz (Eds.), *The EU's external action service: Potentials for a one voice foreign policy*. Innsbruck: Innsbruck University Press.

Lantis, J. S. (2009). Strategic culture: From Clausewitz to constructivism. In J. L. Johnson, K. M. Kartchner, & J. A. Larsen (Eds.), *Strategic culture and weapons of mass destruction: Culturally based insights into comparative national security policymaking*. London/New York: Palgrave Macmillan.

Lawrence, Th. E. (2000). *Seven pillars of wisdom*. London: Penguin Books.

Mahnken, Th. G. (2006). *United States strategic culture*. Washington, DC: SAIC. At https://fas.org/irp/agency/dod/dtra/us.pdf. Accessed 24 Nov 2011.

Nuttall, S. (1992). *European political co-operation*. Oxford/New York: Oxford University Press.

Patton, K. (2010). *Sociocultural intelligence: A new discipline in intelligence studies*. London/New York: Continuum.

Rana, K. S. (2011). *21st century diplomacy: A practitioner's guide*. London/New York: Continuum.

Rettman, A. (2011, April 12). EU intelligence bureau sent officers to Libya. *EU Observer*. At http://euobserver.com/9/32161?print=1. Accessed 14 Apr 2011.

Rettman, A. (2012, June 26). EU builds situation room for Arab League in Cairo. *EU Observer*. At http://euobserver.com/foreign/116757. Accessed 27 June 2012.

Salmon, T. C., & Shepherd, A. J. K. (2003). *Toward a European army: A military power in the making?* Boulder: Lynne Rienner Publishers.

Schneider, B. R., & Post, J. M. (Eds.). (2003). *Know thy enemy: Profiles of adversary leaders and their strategic cultures* (2nd ed.). Maxwell Air Force Base: USAF Counterproliferation Center.

Schrumpf, Ch., & Stam, A. (2012). Non combatant evacuation operations, no way out! *Impetus. Bulletin of the EU Military Staff*, 13, 20–21.

Sjursen, H. (2006). Values or rights? Alternative conceptions of the EU's 'normative' role. In O. Elgström & M. Smith (Eds.), *The European Union's roles in international politics. Concepts and analysis*. London/New York: Routledge.

Smith, M. E. (2004a). Institutionalization, policy adaptation and European Foreign Policy Cooperation. *European Journal of International Relations, 10*(1), 95–136.

Smith, M. E. (2004b). *Europe's foreign and security policy. The institutionalization of cooperation*. Cambridge: Cambridge University Press.

Soetendorp, B. (1999). *Foreign policy in the European Union: Theory, history and practice*. London: Longman.

Sondhaus, L. (2006). *Strategic culture and ways of war*. London/New York: Routledge.

Sorentino, D. (2011). Socio-cultural intelligence. At http://www.brgresearch-group.com/uploads/Article_-_SocioCultural_Intelligence_-_2011_02_10_02.pdf. Accessed 24 Feb 2012.

Stewart, E. J. (2006). *The European Union and conflict prevention: Policy evolution and outcome*. Münster: LIT Verlag.

Tolksdorf, D. (2012). *The role of EU special representatives in the post-Lisbon foreign policy system: A renaissance?* IES Policy Brief no. 2. At http://www.ies.be/files/2012-02%20PB_0.pdf. Accessed 27 Mar 2013.

Walsh, J. I. (2009, April). Security Policy and Intelligence Cooperation in the European Union. Paper prepared for the biennial meeting of the European Union Studies Association, Los Angeles. At http://www.euce.org/eusa2009/papers/walsh_12C.pdf. Accessed 14 May 2012.

CHAPTER 7

Criminal Intelligence in the EU

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

Criminal intelligence cooperation in the EU internal security field is strongly focused on operational activities and their results, and based on concentrated resources and capabilities serving their security interests where they cross national boundaries of jurisdiction. This means that criminal intelligence cooperation is subservient to the legal, institutional and practical regulations designed by Member States to better protect internal security and public order through more effective law enforcement. Hence the strategic intelligence dimension should be conceived as an EU 'overlay' ancillary to Member States' operational arrangements. Its contribution to internal security consists in enabling national law-enforcement authorities to obtain a comprehensive picture of criminal threats and risks located both inside and outside the EU, build situational awareness and work out a strategic response to the major problems and challenges to internal security and public order in the EU.

A. Gruszczak, *Intelligence Security in the European Union*,
DOI 10.1057/978-1-137-45512-3_7

The application of intelligence to the area of internal security, home affairs and criminal justice raises certain methodological reservations. There is a need for a practical and comprehensive conceptualisation of intelligence applicable to both internal security and law enforcement and thus appropriate for the pre-crime framework for analysis adopted in this chapter. Criminal intelligence analysis is a concept which seems to match intrinsic features of twenty-first-century global organised 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 respond proactively to threats and risks posed by organised criminal groups. The steps taken in recent years by EU institutions and agencies, especially the European Council and the Council of the EU, as well as Europol and Frontex, have been leading towards intelligence-led policing, proactive law enforcement and intelligence-driven situation assessment. Criminal intelligence analysis has underpinned EU internal security governance in terms of acquiring knowledge about potential threats, challenges and risks, and working out long-term solutions to tackle them in the most effective way.

The development of criminal intelligence, as observed since the terrorist attacks that hit Europe in the mid-2000s, has contributed to the establishment of an internal security hub encompassing a wide range of institutional, functional, technological and analytical arrangements, applications and solutions. Information exchange, operational assistance and strategic forecast in the internal security hub have been increasingly intelligence driven and involved closer cooperation among national police services and other internal security authorities. The need for accurate information and criminal intelligence has encouraged national authorities to use available EU resources and also contribute with more information and analysis. At the national level, law-enforcement agencies in Member States have adopted intelligence methods and techniques that have expanded the field of intelligence both in the domestic and international domains (Aldrich 2011, p. 20).

This chapter seeks to examine how strategic intelligence at the EU level has contributed to cross-border cooperation in the fields of law enforcement and criminal justice. It highlights the complex network architecture of institutional linkages and puts emphasis on specific elements of intelligence tradecraft adopted in the internal security hub.

The Institutional Framework for Criminal Intelligence Cooperation

Internal security intelligence in the EU combines elements of strategic intelligence with operational intelligence support for national law-enforcement authorities in EU Member States. As an integral component of the EU strategic intelligence community, the criminal intelligence hub has gradually extended its structure, engaging relevant EU agencies and units, and also encouraging external partners (states, organisations) to co-operate in the area of information exchange and sometimes intelligence sharing. In this way dispersed sources of information and analysis have been concentrated around Europol—a single agency recognised by Member States and EU institutions as the central node. Europol has been allocated specific competences as regards information sharing and intelligence production. Simon Robertson (1997, p. 23), former analytical officer at Europol, noted that 'operational intelligence is most effective when it is undertaken as close to an operation as possible, with intelligence analysts working in conjunction with the law enforcement officers involved in the investigation'. This is why since its inception Europol has been seeking to enhance the strategic dimension of its intelligence activities as a prerequisite of a robust, effective and firm operational support for law-enforcement services in Member States.

Operating at the centre of the criminal intelligence hub, Europol has not only developed internal intelligence capabilities focused on strategic intelligence products, but also extended cooperation, exchange and communication mechanisms with other EU bodies, principally Eurojust, Frontex and the EU Intelligence Analysis Centre, concerned with effective internal security governance in the EU. Europol director Rob Wainwright (2012, p. 2) described his agency as 'a multilateral hub for law enforcement cooperation in Europe'.

The present study will focus on the above-mentioned agencies and units, as its scope precludes detailed elaboration of other partners' organisations, functions and roles. Europol was created as a police information unit assisting national police authorities in their fight against transnational organised crime. Its origins can be traced back to 1992, when the Maastricht Treaty provided for police and judicial cooperation in criminal matters. It was stipulated in the Treaty on European Union, Article K.1.9, that a European Police Office (Europol) should be established with the aim of exchanging information within an EU-wide system. At that time, information exchange on major threats to internal security, like terrorism, organised crime and money laundering, was informal and dispersed. The extreme sensitivity of strategic analytical materials and operational information, held as it was by EU Member States, precluded any centralised system of information exchange and intelligence sharing; national authorities responsible for internal security and public order preferred to use secret, informal, bilateral channels and secure communication and information-exchange channels (Deflem 2010, p. 134; Fägersten 2010, p. 506). The Berne Club, a clandestine forum for the exchange of secret intelligence among several Western European countries, emerged in the early 1970s on the initiative of heads of intelligence and counter-intelligence services. The Berne Club set up a special secure telecommunications network enabling rapid information exchange on major terrorist threats (Chevallier-Govers 1999, p. 133; Nomikos 2007, pp. 167–9; Scheren 2009, pp. 175–6). Another network, established in 1977, was the Bureau de Liaison (BdL), which was tasked with facilitating information exchange on terrorist threats and attacks, and with the encrypted transmission of information (Statewatch 1996, pp. 1–2; Balzacq et al. 2006, p. 120).

Europol, as envisaged in the Maastricht Treaty, became fully functional on 1 July 1999. The Convention on the establishment of a European Police Office, signed in 1995,[1] defined Europol's primary objective as the improvement of effectiveness and cooperation by Member States' competent authorities in the prevention and combating of terrorism, drug trafficking and other serious forms of international crime affecting at least two EU countries. Europol was tasked with obtaining, collating, analysing and exchanging information and intelligence as well as preparing threat assessments, strategic analyses and general situation reports relating to its objectives (Deflem 2006, p. 349; Bruggeman 2006, pp. 206–7; Mounier 2009b).

To date Europol has offered a wide range of intelligence products, mostly strategic analyses and assessments, such as SOCTA (Serious and Organised Crime Threat Assessment) and TE-SAT (Terrorism Situation and Trend Report), as well as criminal intelligence deliverables resulting from Analysis Work Files (AWFs). The Analysis Work File 'is the only existing legal tool at European level to simultaneously store, process and analyse factual information ("hard" data) and in particular "intelligence" (or "soft" data), including personal data of a sensitive nature' (Europol 2012). SOCTA encompasses analytical findings based on data available within Europol, especially from appropriate AWFs, supplied by EU

Member States, associated countries and organisations, and supplemented by open sources. TE-SAT is an unclassified report built on Europol's own information, including AWFs, Member States' reports, information provided by third countries and organisations and information gained from open sources. Profiles of new and emerging trends drawn from Europol's SCAN (Scanning, Analysis & Notification) system are also used (Europol 2010).

Europol is also charged with providing strategic intelligence to assist with and promote the efficient and effective use of the resources available at national and EU levels for operational activities, and support for such activities (Europol 1995; Council of the EU 2009c; De Moor and Vermeulen 2010). In Europol's early days there was a lack of clarity as to what strategic intelligence should mean in practice. Analytical Guidelines published in July 2000 (Europol 2000) contained definitions of basic concepts and terms, an overview of the intelligence model, a description of the intelligence cycle, and a presentation of data integration techniques.

Europol's state-of-the-art information and communication system is a multimodal advanced network infrastructure linking the Europol Information System, the central criminal information and intelligence database and the crime reference system for EU law-enforcement and cooperation partners with dedicated thematic data warehouses and cross-reference applications. All databases and services are available 24 hours a day, seven days a week, enabling the fast and secure search, analysis and linking of key information.

Cross-border criminal justice in the EU is coordinated by Eurojust. This agency was set up in 2002 and was preceded by a provisional judicial cooperation unit active since early 2001. It is composed of national prosecutors, magistrates or police officers of equivalent competence. Its objective is to improve coordination of cross-border investigations and prosecutions and cooperation between the competent authorities in Member States in relation to serious and organised crime (Council of the EU 2002, 2009d). The general competence of Eurojust covers the types of crime and offence in respect of which Europol is also competent to act, including organised crime, terrorism, drug trafficking, cybercrime and money laundering (Brammertz 2000, p. 211; Xanthaki 2006, pp. 176–8; Suominen 2008, pp. 220–1). The exchange of criminal justice information is Eurojust's principal activity. Information mostly comes from Member States but it can be also delivered by Eurojust's contact points in third countries, especially those which have concluded cooperation agreements with the agency and appointed liaison prosecutors at Eurojust (Coninsx and Lopes da Mota 2009, p. 168). Eurojust's case management system (CMS), established thanks to the 2008 amendment to the Council decision of 2002 setting up Eurojust, responds to the growing need for a centralised information system to manage the increased amount of information reaching the agency. New competences granted to Eurojust in the 2008 amended decision related to the processing of personal data from individuals suspected of having committed a criminal offence. The system was upgraded in 2014 to improve its operational capabilities and usability (Eurojust 2015, p. 19). The CMS provides operational support by collecting information uploaded by Member States and other relevant partners and processing it for the purposes of ongoing cross-border criminal investigations and prosecutions involving Eurojust as a broker. Information can also be used for strategic analytical projects about certain areas of transnational crime in the EU. A good example is the Strategic Project on Environmental Crime carried out by Eurojust in the period 2013–2014 (Eurojust 2014). Although the project was not intelligence driven and its methodology was not focused on strategic tools and methods, the final outcome resembled the fully fledged situational assessments and analytical reports produced by the major players in the EU intelligence community.

External threats and risks are identified, assessed and reported by Frontex, the EU agency which manages operational cooperation at the external border of Member States. Frontex facilitates and renders more effective the application of existing and future Union measures relating to the management of external borders (Council of the EU 2004c; European Parliament and the Council of the EU 2011). Its tasks are to carry out risk analyses, including the assessment of the capacity of Member States to face threats and pressure at the external borders, and to participate in the development of research relevant for the control and surveillance of external borders (Carrera 2007, pp. 14–17; Leonard 2009, pp. 382–5; Pollak and Slominski 2009, pp. 917–8; Trauner 2012, pp. 793–5; Wolff and Schout 2013, pp. 309–10). Frontex is also responsible for developing and operating information systems enabling 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 the interoperability of systems. More specifically, the agency is tasked with developing and applying a common integrated risk-analysis model.

It prepares both general and tailored risk analyses to be submitted to the Council and the Commission (Council of the EU 2004c).

Frontex also provides intelligence support to the European Border Surveillance System (EUROSUR), an information-exchange framework developed since 2014 to strengthen cooperation between respective national authorities of Member States and with Frontex (European Parliament and the Council of the EU 2013b). EUROSUR provides participating actors with the infrastructure and tools needed to improve their situational awareness and reaction capability at the external borders of the EU. The central element of EUROSUR's information-exchange system is a network of National Coordination Centres (NCCs) established in each Member State. The NCCs collect and process information about a situation at the external border of a given Member State with the aim of creating a national situational picture. They also feed Frontex with relevant information contributing to a European situational picture and a common pre-frontier intelligence picture. These two strategic intelligence products are built on both national inputs transmitted via the NCCs and additional information acquired by Frontex from EU bodies (mainly the EU Satellite Centre and the European Maritime Safety Agency) and collated with knowledge from open sources (Seiffarth 2011).

Other agencies and units include the EU Agency for Network and Information Security, which is in constant touch with Europol's European Cybercrime Centre (EC3), and the European Monitoring Centre for Drugs and Drug Addiction, which analyses emerging trends in addiction and the use and illegal trade of drugs in the EU, as well as producing situational assessments, risk profiles and trend reports.

The diversity, scope, structural complexity and dense networks of the internal security hub are unique features of intelligence cooperation in the EU. While its principal focus is operational intelligence, advances in strategic intelligence, especially in terms of strategic awareness, situational assessment, risk analysis and trend setting, are definitely higher in this segment than in others within the EU intelligence community.

Criminal Intelligence Tradecraft in the EU

Serious and organised crime often has a transnational dimension. Criminal intelligence compiles, analyses and disseminates information for the purposes of anticipating, preventing or surveilling criminal activity (US Department of Justice 2003, p. 54) and can also can provide law-enforcement services with an understanding of crime patterns and trends (Ratcliffe 2008, pp. 6–7). By acquiring information and delivering it to the appropriate judicial authorities in the pre-trial investigation phase, it is often involved in criminal proceedings (Kaiafa-Gbandi 2010, pp. 366–7). In the aftermath of terrorist attacks on the USA (2001), Spain (2004) and the UK (2005), criminal intelligence became closely linked to, and in some areas interconnected with, other intelligence disciplines. EU agencies dedicated to internal security and criminal justice were either in their infancy or not yet in existence. Input from national law-enforcement services was therefore either limited or selective. Moreover, willingness to deliver criminal information and national analytical products to Europol varied considerably among Member States—the result, to a considerable extent, of the tortuous process of building a Europol information system and constant problems with securing information transmitted from national units to Europol. In a nutshell, efforts aimed at encouraging a more intense and effective exchange of criminal information and intelligence had not yielded the expected results, mostly due to the lack of unanimity and the deficit of trust among Member States (Bures 2006, pp. 62–3; Müller-Wille 2006; Duke 2006, pp. 619–20).

EU intelligence tradecraft in the field of internal security has treated intelligence disciplines selectively, depending on the availability of information sources and the ability to extract, collect and collate materials. The political rationale behind intelligence cooperation at Union level precluded EU institutions or agencies from developing a comprehensive cross-discipline system. However, the scourge of terrorism that hit the EU in the 2000s gave rise to an important modification of the cooperative framework among the law-enforcement authorities of Member States.

The sense of resilience to the most serious threats was lost in the aftermath of the 11 March 2004 terrorist attack in Madrid (Gruszczak 2013, p. 22). EU institutions called for the improvement of mechanisms for cooperation and the promotion of effective systematic collaboration between police, security and intelligence services of Member States. 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 2005, p. 9). Accordingly, EU institutions and Member States highlighted the relevance of information exchange and intelligence sharing for an effective counter-terrorism strategy and operational coordination between national law-enforcement authorities. But it was the terrorist attacks in London in July 2005 that motivated Member States to take up the issue of criminal intelligence capabilities at the EU level (Fägersten 2010, pp. 511–2). A British proposal submitted to EU interior ministers gathered at an informal meeting in September 2005 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).

The original concept of European criminal intelligence took the form of an intelligence cycle which relied on inputs from Europol and Member States contributing either directly or through appropriate institutional or working schemes as provided in EU law. The elements of that cycle were the following:

- setting strategic priorities on the basis of threat assessments delivered by appropriate EU bodies, mainly Europol;
- identifying knowledge gaps;
- producing intelligence requirements, facilitated by Europol;
- launching a proactive collection programme in Member States;
- storing and analysing intelligence in Europol;
- producing specialist threat assessments to improve knowledge in priority areas;
- identifying top criminals and networks;
- targeting top criminals and networks by Member States;
- recycling through Europol intelligence generated by investigations underway (Council of the EU 2006b, p. 3).

This cycle required operational excellence and demanded full commitment from national stakeholders (law-enforcement agencies of Member States) to the principles of EU criminal intelligence cooperation and a strong capacity to deliver the information and data requested. This was a highly demanding task and not every Member State was ready, able and willing to meet these requirements. As a result, the European Criminal Intelligence Model did not achieve full working capacity, nor was it grounded in a comprehensive approach to intelligence tradecraft.

A new strategic approach, the EU Internal Security Strategy (EU ISS), adopted in early 2010, sought to further improve security in the EU, protect the safety of the citizens of the Union and tackle organised crime, terrorism and other threats. Building on some of the original premises of the ECIM, the new strategy focused on an intelligence-led, proactive approach to the challenges of terrorism, organised crime and both natural and man-made disasters. It called on Member States to foster information exchange on a basis of mutual trust and share intelligence in a timely manner in compliance with the principle of information availability (Council of the EU 2010c). The authors of a study on the EU ISS submitted to the LIBE committee of the European Parliament stressed that: 'The central articulation of the guidelines is between the emphasis on a proactive, intelligence-led approach, and the development of a comprehensive model for information exchange and operational cooperation' (Scherrer et al. 2011, p. 32).

The Internal Security Strategy, overwhelmingly accepted as a viable political option, offered a strategic framework and broad guidelines for a comprehensive approach to effective intelligence-led policing and enhanced evidence-based criminal intelligence cooperation among EU Member States with the direct and active involvement of competent EU agencies and bodies (Bossong and Rhinard 2013, pp. 51–2; Horgby and Rhinard 2013). As a follow-up to the post-Lisbon reconfiguration, in mid-2010 the Belgian presidency launched a proposal to transform ECIM into the core element of a multi-annual policy cycle for organised and serious international crime on the basis of an intelligence-led policing approach. In November 2010 the JHA Council adopted conclusions on the creation and implementation of an EU-wide policy cycle to be rolled out in two stages: an initial two-year policy cycle 2011–2013 and a fully fledged four-year policy cycle 2013–2017 (Council of the EU 2010d).

Despite its name, the cycle was rather conceived as a temporally determined sequence of strategic assessments, political decisions and operational plans intended to bring about a better systemic response to current and emerging threats (Council of the EU 2010d). The policy cycle could thus be understood as the linear development of a proactive, vertically oriented, problem-oriented and comprehensive approach to organised and serious international crime, tackled at the EU level with the active involvement of competent EU institutions and agencies. Europol's Organised Crime Threat Assessment was the point of departure both for the initial cycle and the subsequent, fully fledged cycle. This meant that ECIM's intelligence-led orientation and threat assessment methodology underpinned and permeated the logic of the EU policy cycle for organised and serious international crime.

ECIM adopted a centralised architecture, with Europol as the 'central EU capability to receive, store and analyse this collected information' (Council of the EU 2010d) intended to support the operational activities of Member States based on its previous strategic assessments. The application of ECIM was predetermined by Europol's capabilities, which had been reduced by legal provisions and organisational schemes, as well as Member States' inability to exercise joint will or to welcome advanced cooperation over information and intelligence exchange in the area of transnational criminal justice. Europol, equipped with enhanced information management, and intelligence production and sharing capabilities, assumed the role of an EU criminal information node and the centre for law-enforcement expertise (Busuioc et al. 2011; Carrapiço and Trauner 2013, pp. 366–8). Most importantly, Europol was tasked with leading the further development of ECIM, to include a common EU approach to the targeted collection and sharing of key criminal information, the integrated analysis of financial intelligence linked to all crime phenomena, and the identification of top criminal targets. It was also to improve and strengthen Organised Crime Threat Assessment (OCTA) methodology and promote ECIM principles among national authorities in the Member States as well as EU institutions and agencies (Europol 2009a). The EU ISS also gave Europol responsibility for analysing future situations and scenarios and for preparing regular threat assessments.

The original policy cycle for serious international and organised crime established by the Council in 2010 consisted of four stages. For the purposes of criminal intelligence, the policy cycle included:

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

The Council decided that the initial two-year cycle should focus on crime priority areas designated by the Standing Committee on Internal Security (COSI), and be based on the traditional Europol methodology employed in the OCTA assessments and organised within the revised COSPOL framework, which concentrated on single law-enforcement issues rather than applying an integrated approach (Council of the EU 2010d).

The next, fully fledged four-year cycle started with the new SOCTA assessment produced by Europol on the basis of a new methodology. This assumed an integrated approach, engaging various categories of stakeholder: EU institutions (Council, Commission), EU agencies and bodies (Europol, Frontex, INTCEN) and Member States (relevant national criminal intelligence or law-enforcement services). It supported Member States to implement national intelligence models by delivering training packages and streamlining the specialised courses offered by the European Police College. It put greater emphasis on reporting and independent evaluation mechanisms.

In concentrating on serious international and organised crime, the policy cycle has sought to effectively implement ECIM in its most practical meaning, thus gaining leverage in the overall EU strategy in the area of freedom, security and justice. However, in order to be productive and efficient, it has to incorporate dispersed elements of the methodological process accelerated by post-Lisbon developments in the field of EU internal security.

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. Vidalis (2003, p. 5) conceives of a threat assessment as a statement of threats in relation to the vulnerabilities of a given entity and to agents of threat (hostile states, terrorist groups, criminal organisations, irregular migrants); it is also a statement of the capabilities that those agents are believed to possess. Threat assessment is of a somewhat qualitative nature (Gill 2010); it takes into account numerous categories of data delivered by authorised stakeholders or extracted from open sources.

In response to the British proposal of a European Criminal Intelligence Model, the Council of the EU decided to develop intelligence-led policing and the Organised Crime Threat Assessment (Council of the EU 2005c). Europol was to produce OCTA annual reports in close cooperation with Member States, which would transmit information and intelligence as required by Europol and issued through the heads of its national units. Europol would also communicate those requirements to EU agencies and bodies and to third countries and organisations with which it had cooperation agreements. Through Europol the EU sought to build its own capacity to deliver to EU and national stakeholders independent evaluations of threats from terrorism and organised criminality (Argomaniz 2009a, p. 160).

In 2006, the first Organised Crime Threat Assessment was published by Europol, replacing the Organised Crime Report prepared annually since 1993. The then director of Europol, Max-Peter Ratzel, described the OCTA as 'a core product of the intelligence-led policing concept' (Europol 2006, p. 3). The report stated that: 'The OCTA, being a forward-looking document, will help decision makers 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, p. 4).

Intelligence tradecraft employed in the OCTA was described in brief: '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, p. 4). Methodology was the Achilles' heel of those yearly reports and this gave rise to criticism on the part of experts and practitioners (van Duyne 2007; Zoutendijk 2010) 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 an intelligence-led approach.

In a follow-up to the EU Internal Security Strategy, the Council called for the preparation of the European Union Serious and Organised Crime Threat Assessment (EU SOCTA) on the basis of a new methodology (Council of the EU 2010f) 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. The first such assessment was published by Europol in March 2013 (Europol 2013). In general the SOCTA methodology follows the typical intelligence cycle, focusing both on the delivery capabilities of major contributors (i.e. Europol and Member States' law-enforcement services) and the previously agreed customer requirements. The fundamental feature of the SOCTA is its anticipation of organised transnational criminality: 'The SOCTA is a present- and future-oriented threat assessment. It goes a step further than a situation report (which is retrospective and mainly statistical) as it takes into account possible future developments' (Council of the EU 2012b, p. 4). SOCTA methodology includes a watchlist 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 conjunction with the SOCTA expert group (composed of EU Member States, Europol's non-EU partner countries and organisations, the European Commission and the Council's General Secretariat), consists of four steps: focus, tools, analysis and assessment, and results. It begins with three focus points: organised criminal groups; serious and organised crime areas; and the environment upon which they have an effect and by which they are facilitated. These elements are assessed using three types of indicators and additional crime-relevant factors. The latter are facilitating factors and vulnerabilities in the environment that have an influence on current and future opportunities or barriers to 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 through a Delphi exercise.

The analysis and assessment reflects the very structure and organisation of Europol and the police cooperation network centred on this agency. The analytical work starts by accessing the resources held by Europol which are catalogued and stored in Analysis Work Files. These may be combined with threat notices on new and emerging trends, specific threat assessments and other strategic reports developed at Europol. Additionally, open-source 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 concluded strategic or operational agreements with Europol.

The core part of the analysis cycle is the processing of the data received from stakeholders and acquired from open sources, and the assessment of indicators and crime-relevant factors. Adopting a holistic approach, Europol aims to connect the available data sets and detect 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 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 2012b).

The new criminal intelligence product offered by Europol is much more advanced and substantial than its predecessor. First, the tradecraft employed in the SOCTA analysis cycle is more developed and clearly highlights potential future trends and issues (Europol 2013). It mines a considerable amount of information and data acquired from a variety of sources. Second, it has introduced methods, tools and techniques typical of criminal intelligence models implemented by leading countries, within and beyond Europe. Finally, the threat assessment methodology embedded in the SOCTA seems to be a good benchmark, or even best practice, for Member States that lag behind the leading countries in terms of intelligence capabilities and information management. EU criminal intelligence tradecraft may encourage them towards more intense and productive cooperation with Europol in the exchange of information and criminal data.

The SOCTA is a considerable step forward in the development and enrichment of EU criminal intelligence tradecraft. It does not mean, however, that this product perfectly fits the intelligence-led approach to internal security of the European Union. The methodology is still behind the state-of-the-art applications employed by global powers. The final product still depends much on 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, the intelligence analysis carried out by this agency often falls short of the expectations of practitioners, especially national intelligence officials in Member States. Following SOCTA methodology, crime matrices and cognitive maps could be created, although so far, and with reference to the first ever SOCTA report published in 2013, no hard evidence of such an advanced proactive approach on the part of Europol exists. Nevertheless, the SOCTA proves the qualitative potential of Europol and its ability to take advantage of diverse elements of criminal intelligence tradecraft.

The EU Terrorism Situation and Trend Report (TE-SAT) is another flagship strategic intelligence product based on threat assessment methodology. The report includes an overview of terrorist activities throughout the EU against a global backdrop and a typology of terrorist organisations by their source of motivation (religious, ideological, ethno-nationalist) and predominant trends.

TE-SAT was established after 9/11 as a reporting mechanism from the Council's Terrorism Working Party (TWP) to the European Parliament. In 2006 a new methodology was approved by the Council and the TWP was replaced by Europol. TE-SAT is built on Member States' input, information and analysis from some EU agencies and entities (Eurojust, Frontex, EU Counter-Terrorism Co-ordinator, INTCEN), reports from non-EU partners and information acquired from open sources. Member States are obliged to collect information resulting from criminal investigations into terrorist crimes conducted by national law-enforcement authorities. They decide whether a given piece of information should be transmitted to Europol. Any information delivered by a relevant national stakeholder to Europol is verified, processed by Europol and cross-checked with Member States. Any individual Member State may question Europol's output if an error, misinterpretation or gap is identified. In such a case Europol should correct, complement or improve the results of its intelligence work and then return it to Member States for validation (Europol 2015a, p. 47).

A separate procedure was established for contributions from EU agencies and units, which may send their products directly to Europol's unit in charge of TE-SAT or, as is the case for Eurojust, feed information to AWFs Eurojust is associated with and which are later explored in the preparatory work for a new TE-SAT (Bures 2011, pp. 122–3; Weyemberg et al. 2014, p. 16). Moreover, the Europol-Eurojust working group established on the basis of the 2010 inter-agency agreement can also engage its experts in information exchange for the purpose of terrorism situation assessment (Boehm 2012, pp. 326–8). Apparently, a similar agreement was reached in 2005 between Europol and SITCEN. This agreement has not been disclosed but EU officials have acknowledged on many occasions that such cooperation exists and creates a certain positive impact on TE-SAT contents (Biegaj 2009, pp. 50, 56–7; Bures 2011, p. 53).

The Risk-Analysis Model

Risk analysis is a tool widely used to understand problems and identify challenges and hazards in many areas of contemporary life, especially under conditions of uncertainty (Frenkel et al. 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 the skills, measures and technologies employed to estimate the sources and types of risk identified, assess the probability of their appearance and work out appropriate solutions at the EU level. While criminal intelligence focuses on serious threats generated by domestic and transnational organised groups, risk analysis is more oriented to 'soft' threats, which do not undermine the foundations of public order, the rule of law or state authority but may produce long-term negative consequences for systemic stability, public accountability and the reliability of state institutions. Criminal intelligence can be said to address the problem of legal order, while risk analysis relates to societal trust and the legitimacy of the state's authority. Generally, risk analysis is concerned with the ideological, legal, human and systemic prerequisites of freedom, security and justice in the EU. Most of all, risk analysis serves to identify 'precautionary regions' or 'danger zones' (Jablonowski 2006, pp. 42–3), reduce uncertainty and contribute to effective solutions adopted by EU institutions or agencies.

Obviously, the EU's external border zones have been one of the most sensitive 'precautionary areas' for EU Member States and their citizens, with significant exposure to illegal migration and asylum seeking which have resulted in an immigration and asylum legal agenda as well as the development of an integrated border management system aiming to reinforce the EU's 'external shield' and reduce the probability of risk-prone transfers of persons and goods into the territories of Member States. One element of an exclusionary approach to immigration and asylum was the establishment of Frontex, with one of its principal tasks being to carry out risk analyses, including the assessment of the capacity of Member States to face threats and pressure at the external borders. Reliable data and the capacity to convert it into an intelligence report is highly relevant to Frontex's utility and identity,[2] but statistical data it receives from Member States directly about the intensity of migratory movements is often sparse, scattered and divergent in terms of methodology. Frontex and EU Member States have therefore sought to integrate various forms of intelligence and risk analysis using interconnected information sources and data sets dedicated to continuous or emerging security-related issues. Frontex has been endowed with certain competences regarding information management. Member States are obliged to provide the agency with all necessary information regarding the situation and possible threats at the external borders, and EU bodies, public media and other open sources are also used. Most importantly, in the interests of the security of Member States the amended Frontex regulation authorises the agency to collect and process the personal data of individuals involved in its operational activities, such as joint return operations, pilot projects and rapid interventions at the external borders. Collated information, including personal data, is further processed for strategic and operational purposes and contributes to the analytical and operational work of other EU law-enforcement agencies, mainly Europol.

Risk analysis is key to Frontex's intelligence tradecraft. As the starting point of all Frontex operational activities, it fits the logic of the analysis cycle and delivers a picture of the situation at the EU's external borders, contributing to training activities and responding to the needs of its principal customers—EU agencies and Member States. The Risk Analysis Centre was set up in 2003 as a strategic intelligence tool for the Strategic Committee on Immigration, Frontiers and Asylum within the JHA Council of the EU. CIRAM—the Common Integrated Risk Analysis Model—is based on a six-field matrix, bringing together elements of criminal intelligence and risk assessment (Carrera 2007, pp. 15–16). It was updated in 2011 to better respond to the changing external environment of the EU, to deal effectively with new types of risk and threat and to reflect 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, p. 11).

The current management approach of CIRAM defines risk as a function of its threat, vulnerability and impact (Frontex 2013a, p. 11). Operationally, CIRAM supports the coordination of joint operations at the external borders conducted or coordinated by Frontex. It provides a background picture of conditions, determinants and circumstances in the area of a planned joint operation. 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 and the *modi operandi* of criminal groups or smuggling networks operating in the area of Frontex's planned activities.

Operational analytical products are based on a proactive assessment of a security environment, including anticipation of threats and hazards and early warning, with knowledge management and risk analysis underpinning strategic analysis. CIRAM, in responding to the needs of decision makers in Member States, officials in EU institutions and agencies, border authorities and international organisations, relies for its effectiveness and reliability on a four-tier access control model that involves gathering information from numerous sources dispersed over the territory of Member States. To this end, the Frontex Risk Analysis Network (FRAN) was established in 2007. It provides a 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, feeds Frontex's Risk Analysis Unit (RAU) with data which are processed, analysed and disseminated in the form of analytical products. The most important are quarterly, semi-annual and annual risk analyses. The RAU also issues occasional documents and other tailored risk-analysis products.

The Frontex risk analysis model reflects the EU's proactive approach to public order and internal security. The pre-crime perspective addresses not only 'crimes of arrival', such as inflow of irregular migrants seeking refugee status, it also deals with the problem of increasing criminality by transnational organised criminal networks involved in people trafficking. This is why Frontex's methodology combines quantitative risk analysis, which uses 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 a cost–benefit approach to EU immigration and asylum policies.

Conclusions

Organised crime reflects a dynamic transition from individual, locally based criminality to transnational organised serious crime with powerful resources and global reach. It is from this phenomenon that criminal intelligence has developed, with EU criminal justice and home affairs institutions adopting responsibility for legal instruments and measures in this area. The Council of the EU, in integrating the ECIM with the policy cycle for organised and serious crime, sought to tackle organised criminality in a more efficient and proactive way through a comprehensive threat assessment and by translating identified goals into operational activities.

The effective use of intelligence remains the domain of national law-enforcement services and their ability to prevent and combat criminal groups. However, the efficiency of criminal proceedings should take into account not only the operational aspects of law enforcement in a given Member State but also some organisational prerequisites emerging at supranational level and embedded in general consensual strategies and operational plans. The EU criminal intelligence model helps develop strategic blueprints for tackling current internal security problems and prepare for anticipated threats and hazards. It also offers national authorities the practical knowledge required for effective management of their resources. Its four dimensions—technological harmonisation, legal approximation, cultural exchange and centralisation of information exchange—are envisaged in the policy cycle, enabling a more effective and better organised framework of criminal intelligence in the EU.

The intelligence-led policing and criminal intelligence model, which requires genuine inter-governmental cooperation and credible information exchange, demonstrates that EU institutions and agencies are responding to demands from individual Member States to improve the management of the sensitive information and criminal data they supply.

The intelligence process, however, remains decentralised and subject to national predilections and habits, or national security cultures, which quite often restrict the scope for intelligence cooperation at the EU level. The implementation of the EU policy cycle for organised and serious international crime is important because it is the first time a common framework for criminal intelligence tradecraft has enabled both Member States and EU agencies and institutions to more effectively deliver valuable inputs and obtain valuable and useful outcomes, crucial for the prospects of robust, effective and legitimate intelligence cooperation in the realm of EU internal security.

So far, the intelligence products offered by EU agencies are fairly useful although they suffer from restrictions imposed by individual Member States on the transmission of the sensitive information and raw material they possess. In addition to Europol's SOCTA and TE-SAT or Frontex's FRAN reports, there are numerous tailored analyses addressing specific requests from consumers, especially regarding prevention, anticipation and foreknowledge of the most serious threats, risks and perils. These products seek to satisfy the strategic and operational needs of law-enforcement services in Member States, and to develop and widen the cognitive capabilities of the emerging EU intelligence community.

All-source analysis within the EU intelligence community is still the frame of reference. There are too many loopholes in intelligence workflow hindering the proper use of sources and materials available to EU actors. Nonetheless, some attempts have been made to integrate dispersed sources and enhance national inputs to the intelligence process unfolding in certain fields of EU security policy, and strategic intelligence in particular is seeing an expanding flow of information and data originating in varied sources of EU intelligence cooperation. Recent years have seen increased use 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 warnings of potential and substantial threats and dangers. The EU can and should convince its Member States and external partners of the utility, relevance and appropriateness of strategic intelligence. The continuous improvement in criminal analysis at the EU level is an argument for the further enhancement of an intelligence-led approach to EU internal security governance.

Notes

1. The Convention was replaced by the Council decision of 6 April 2009 (Council of the EU 2009c).
2. An anonymous Frontex official, interview, December 2012.

Bibliography

Aldrich, R. J. (2011). Global intelligence co-operation versus accountability: New facets to an old problem. In L. Scott, R. G. Hughes, & M. S. Alexander (Eds.), *Intelligence and international security. New perspectives and agendas*. London/New York: Routledge.

Argomaniz, J. (2009a). Post-9/11 institutionalisation of European Union counter-terrorism: Emergence, acceleration and inertia. *European Security, 18*(2), 151–172.

Balzacq, Th., Bigo, D., Carrera, S., & Guild, E. (2006). The treaty of Prüm and EC treaty: Two competing models for EU internal security. In Th. Balzacq & S. Carrera (Eds.), *Security versus freedom?: A challenge for Europe's future*. Aldershot/Burlington: Ashgate.

Biegaj, A. (Ed.). (2009). *Ten years of Europol, 1999–2009*. The Hague: European Police Office.

Boehm, F. (2012). *Information sharing and data protection in the area of freedom, security and justice. Towards harmonised data protection principles for information exchange at EU-level.*. Berlin/Heidelberg: Springer-Verlag.

Bossong, R., & Rhinard, M. (2013). The EU internal security strategy. Towards a more coherent approach to EU security? *Studia Diplomatica, LXVI*(2), 45–58.

Brammertz, S. (2000). Eurojust: parquet européenne la première generation? In G. de Kerchove & A. Weyembergh (Eds.), *Vers un espace judiciaire pénal européen*. Bruxelles: Editions de l'Université de Bruxelles.

Bruggeman, W. (2006). A vision on future police cooperation with a special focus on Europol. In J. W. de Zwaan & F. S. N. J. Goudappel (Eds.), *Freedom, security and justice in the European Union: Implementation of the Hague programme*. The Hague: T.M.C. Asser Press.

Bures, O. (2006). EU counterterrorism policy: A paper tiger? *Terrorism and Political Violence, 18*(1), 57–78.

Bures, O. (2011). *EU counterterrorism policy: A paper tiger?* Farnham/Burlington: Ashgate.

Busuioc, M., Curtin, D., & Groenleer, M. (2011). Agency growth between autonomy and accountability: The European Police Office as a 'living institution'. *Journal of European Public Policy, 18*(6), 848–867.

Carrapiço, H., & Trauner, F. (2013). Europol and its influence on EU policymaking on organized crime: Analyzing governance dynamics and opportunities. *Perspectives on European Politics and Society, 14*(3), 357–371.

Carrera, S. (2007). *The EU border management strategy. FRONTEX and the challenges of irregular immigration in the Canary Islands.* CEPS Working Document No. 261. Brussels: CEPS.

Chevallier-Govers, C. (1999). *De la coopération à l'intégration policière dans l'Union européenne*. Bruxelles: Bruylant.

Coninsx, M., & Lopes da Mota, J. L. (2009). The international role of Eurojust in fighting organized crime and terrorism. *European Foreign Affairs Review, 14*(2), 165–169.

Council of the EU (2002, March 6). Council decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime. *Official Journal of the European Communities, L 63.*

Council of the EU (2004c, November 25). 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.*

Council of the EU (2005c, September 29). Council decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences. *Official Journal of the European Union, L 253.*

Council of the EU (2006b, October 10). Comprehensive Operational Strategic Planning for the Police (COSPOL), doc. 5859/4/06 REV 4.

Council of the EU (2009d, June 4). Council decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime. *Official Journal of the European Union, L 138.*

Council of the EU (2010d, September 3). EU policy cycle, 12657/1/10 REV 1.

Council of the EU (2010e, July 5). Expert group—EU policy cycle, doc. 11814/10.

Council of the EU (2010g December 3). 3051st Council meeting Justice and Home Affairs. Press Release, doc. 16918/10, Brussels.

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

Deflem, M. (2006). Europol and the policing of international terrorism: Counter-terrorism in a global perspective. *Justice Quarterly, 23*(3), 336–359.

Deflem, M. (2010). *The policing of terrorism: Organizational and global perspectives.* New York/Abingdon: Routledge.

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

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

Eurojust (2014). *Strategic project on environmental crime. Report.* The Hague: Eurojust.

Eurojust (2015). *Annual report 2014.* The Hague: Eurojust.

European Council (2005, March 3). The Hague programme: Strengthening freedom, security and justice in the European Union. *Official Journal of the European Union, C 53.*

European Parliament and the Council of the EU (2011, November 22). 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.*

European Parliament and the Council of the EU (2013b, November 6). Regulation (EU) no 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur). *Official Journal of the European Union, L 295.*

Europol (1995). Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention). *Official Journal of the European Communities,* C 316, 27 November.

Europol. (2000). *Analytical guidelines.* The Hague: Europol.

Europol. (2006). *EU organised crime threat assessment 2006.* The Hague: Europol.

Europol (2009a). *Europol strategy 2010–2014*. EUROPOL Management Board, doc. 1424-73r1, 2 November.

Europol (2010). Europol launches scan system for strategic notices on newly identified organised crime threats, 1 January. At https://www.europol.europa.eu/sites/default/files/publications/2010-oc-scan-threat-notice-open-version.pdf. Accessed 11 Jan 2010.

Europol (2012). *New AWF concept. Guide for MS and third parties*, doc. Europol no. 525188v14, 31 May.

Europol. (2013). *SOCTA 2013. EU serious and organised crime threat assessment*. The Hague: European Police Office.

Europol. (2015a). *TE-SAT 2015*. The Hague: European Police Office.

Fägersten, B. (2010). Bureaucratic resistance to international intelligence cooperation—The case of Europol. *Intelligence and National Security, 25*(4), 500–520.

Frenkel, M., Hommel, U., & Rudolf, M. (Eds.). (2005). *Risk management. Challenge and opportunity* (2nd ed.). Berlin/Heidelberg: Springer.

Frontex. (2013a). *Annual risk analysis 2013*. Warsaw: Frontex Risk Analysis Unit.

Frontex (2013b). *Strategic analysis*. At http://frontex.europa.eu/intelligence/strategic-analysis. Accessed 27 May 2014.

Gill, P. (2010). Integrated terrorist threat assessment in Europe: An overview. In Belgian Standing Intelligence Agencies Review Committee (Ed.), *Fusion centres throughout Europe. All-source threat assessments in the fight against terrorism*. Antwerp/Oxford/Portland: Intersentia.

Gruszczak, A. (2013). EU intelligence-led policing: The case of counter-terrorism cooperation. In M. O'Neill, K. Swinton, & A. Winter (Eds.), *New challenges for the EU internal security strategy*. Newcastle upon Tyne: Cambridge Scholars Publishing.

Houben, M. (2005). *International crisis management: The approach of European states*. Abingdon/New York: Routledge.

Kaiafa-Gbandi, M. (2010). Harmonisation of Criminal Procedure on the Basis of Common Principles. The EU's Challenge for Rule-of-Law Transnational Crime Control. In C. Fijnaut & J. Ouwerkerk (Eds.), *The Future of Police and Judicial Cooperation in the European Union*. Leiden-London: Martinus Nijhoff Publishers.

Jablonowski, M. (2006). *Precautionary risk management. Dealing with catastrophic loss potentials in business, the community and society*. Basingstoke/New York: Palgrave Macmillan.

Leonard, S. (2009). The creation of FRONTEX and the politics of institutionalisation in the EU external borders policy. *Journal of Contemporary European Research, 5*(3), 371–388.

Löfstedt, R. E. (2005). *Risk management in post-trust societies*. Basingstoke/New York: Palgrave Macmillan.

Mounier, G. (2009b). Europol: A new player in the EU external policy field? *Perspectives on European Politics and Society, 10*(4), 582–602.

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

Nomikos, J. M. (2007). Transatlantic intelligence cooperation, the Global War on terrorism, and international order. In Y. A. Stivachtis (Ed.), *International order in a globalizing world*. Aldershot/Burlington: Ashgate.

Norman, T. L. (2010). *Risk analysis and security countermeasure selection*. Boca Raton/London/New York: CRC Press.

Pollak, J., & Slominski, P. (2009). Experimentalist but not accountable governance? The role of Frontex in managing the EU's external borders. *West European Politics, 32*(5), 904–924.

Power, M. (2007). *Organized uncertainty. Designing a world of risk management*. Oxford: Oxford University Press.

Ratcliffe, J. H. (2008). *Intelligence-led policing*. Cullompton/Portland: Willan Publishing.

Robertson, S. (1997). Intelligence-led policing: A European Union view. In A. Smith (Ed.), *Intelligence-led policing. International perspectives on policing in the 21st century*. Lawrenceville: IALEIA.

Scheren, M. (2009). Vernetzte Sicherheit—Zusammenarbeit der Inlandsnachrichten- und Sicherheitsdienste in Europa. In T. Jäger & A. Daun (Eds.), *Geheimdienste in Europa: Transformation, Kooperation und Kontrolle*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Scherrer, N., Jeandesboz, J., & Guittet, P.-E. (2011). *Developing an EU internal security strategy, fighting terrorism and organised crime*. Brussels: European Parliament.

Seiffarth, O. (2011). The development of the European Border Surveillance System (EUROSUR). In J. P. Burgess & S. Gutwirth (Eds.), *A threat against Europe? Security, migration and integration*. Brussels: VUBPRESS.

Statewatch (1996). EU whatever happened to the Trevi network? *Statewatch Bulletin, 6*(3), 1–2.

Suominen, A. (2008). The past, present and the future of Eurojust. *Maastricht Journal of European and Comparative Law, 15*(2), 217–234.

Trauner, F. (2012). The European Parliament and agency control in the Area of Freedom, Security and Justice. *West European Politics, 35*(4), 784–802.

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.

US Department Of Justice (2003). *National criminal intelligence sharing plan*. Washington, DC: US Department of Justice, Office of Justice Programs. At http://www.cops.usdoj.gov/files/ric/CDROMs/LEIntelGuide/pubs/National_Criminal_Intelligence_Sharing_Plan.pdf. Accessed 14 May 2013.

Van Duyne, P. C. (2007). OCTA 2006: The unfulfilled promise. *Trends in Organised Crime, 10*(2), 120–128.

Vellani, K. H. (2007). *Strategic security management. A risk assessment guide for decision makers*. Amsterdam: Elsevier.

Vidalis, S. (2003). *A critical discussion of risk and threat analysis methods and methodologies*. At http://www.comp.glam.ac.uk. Accessed 27 Apr 2014.

Wainwright, R. (2012, June). *The future of the EU internal security after 2014: Will the UK remain a major player?*. Speech at the European Institute, University College of London. At http://www.ucl.ac.uk/european-institute/highlights/europol. Accessed 13 June 2012.

Weyemberg, A., Armada, I., & Brière, C. (2014). *The inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area*. Brussels: European Parliament.

Wolff, S., & Schout, A. (2013). Frontex as agency: More of the same? *Perspectives on European Politics and Society, 14*(3), 305–324.

Xanthaki, H. (2006). Eurojust: Fulfilled or empty promises in EU criminal law? *European Journal of Law Reform, VIII*(2/3), 175–197.

Yoe, C. (2012). *Primer on risk analysis. Decision making under uncertainty*. Boca Raton: CRC Press.

Zoutendijk, A. J. (2010). Organised crime threat assessments: A critical review. *Crime, Law and Social Change, 54*(1), 63–86.

CHAPTER 8

External Dimensions of EU Intelligence Cooperation

EU intelligence cooperation has been shaped in a global context of increasing transnational threats, external pressures and global risks, but it has also produced opportunities and benefits. Cooperation with non-EU partners (states and organisations) in the context of the EU's overall security strategy was considered meaningful in political and organisational terms. However, the need for practical cooperation and effective exchange of information and intelligence was formulated in vague terms subject to legal and formal barriers, with cooperation with third countries varying widely in scope (Monar 2011, pp. 413–5). In the intelligence security framework, EU institutions and bodies were more eager to gain access to information and intelligence from external partners than to win the practical support and assistance necessary for operational activities. The preventive and anticipatory function of intelligence in the EU developed after the 9/11 terrorist attack and was strengthened in the aftermath of the terrorist bombings in Madrid in 2004 and London in 2005. Unlike terrorist or criminal threats, military risks and crisis-prone phenomena were handled at an operational level, and were subject to specific political and institutional arrangements providing an important role for external actors, most of all NATO and the United States. Military intelligence has been a sensitive and controversial issue and its use for operational and tactical purposes confined to established tasks and agreed actions. Strategically, the European Union has been much more interested in drawing a full

A. Gruszczak, *Intelligence Security in the European Union*,
DOI 10.1057/978-1-137-45512-3_8

picture of its security environment, for which external information and analytical input are required.

One has to bear in mind that horizontal EU-level intelligence networks function in institutionalised hubs engaging relevant agencies and specialised units. Vertical, bottom-up government-led intelligence structures are much less involved in EU-led undertakings. Only the express consent of Member States allows national information and intelligence sources to be involved in cooperation at the EU level. The transnational dimension of the EU intelligence community entails formal agreements, institutionalised arrangements and established practices of information exchange with non-EU actors. Informal settings, tacit agreements and ad hoc deals, however, provide channels, mechanisms and tools of cooperation which are rarely revealed to the public.

The agreements and arrangements concluded by the EU and its external partners were founded on the four main principles underlying mutual obligations:

- protection and safeguarding of classified information;
- ensuring that classified information subject to exchange or delivery meets mutual security clearance rules;
- use of classified information exclusively for the purposes established by the originator;
- prohibition of disclosure of such information to third parties without the clear prior consent of the originator (Koutrakos 2015, pp. 407–8).

The EU's security strategy and policy is embedded in the North Atlantic alliance. Military operations and external crisis management under the CSDP depend largely on NATO's capabilities and equipment, especially in the information and intelligence fields. From the strategic perspective NATO assets, resources and capabilities are useful to EU security policy. The United States as the leading NATO ally—and for a long time the 'security provider' for EU Member States—has had a far-reaching impact on EU intelligence cooperation, particularly in the aftermath of 9/11. The global coalition, with the USA and its European allies at the core, strengthened transatlantic cooperation in the fight against terrorism and related serious criminal activities, such as the financing of terrorism, illegal trafficking in arms and cyber-criminality. Information sharing, including the exchange of personal data, has become the critical element in transatlantic intelligence cooperation, provoking a lively debate in the EU around privacy and personal data protection.

A number of non-EU countries are actively involved in EU security and intelligence cooperation. Norway, Iceland and Switzerland have been long-term participants in both external military and internal security aspects of EU-led security policies and arrangements. The fact that all these countries are part of the Schengen area has established patterns and mechanisms of internal security cooperation, including information exchange and criminal intelligence sharing. The membership of Norway and Iceland in NATO provides a connection with a common platform for military intelligence cooperation with other EU countries belonging to the alliance. Norway has been actively associated with the EU CSDP, participating in missions (police mission in Bosnia) and contributing with personnel and equipment to the CSDP Rapid Reaction Force and to the EU Nordic battle group. Switzerland has taken part in several EU missions and operations for civilian crisis management in Kosovo, Bosnia and Mali. In the area of internal security, these three countries actively cooperate with the relevant EU agencies, namely Europol and Eurojust. They also provide substantial input to terrorism analysis and assessment. Switzerland and Norway have for a long time been active members of informal intelligence cooperation and information-exchange schemes, such as the Berne Club or the Police Working Group on Terrorism, and should therefore be treated as part of the EU intelligence community rather than as external associates.

This chapter analyses three circles of external intelligence cooperation. The first is the NATO alliance, due to its enormous impact on EU CSDP capabilities. Although intelligence sharing between the EU and NATO is severely limited it is, nonetheless, important in strategic terms for the building of situational awareness and military crisis management. Second, the United States' position is peculiar not only because of its leadership of NATO, but also due to its impact on EU internal security and its desire to build 'transatlantic homeland security'. The third circle revolves around EU agencies in charge of criminal intelligence and internal security cooperation that have developed institutional arrangements with numerous non-EU states and international organisations, enabling access to information on and analyses of international crime and global risks.

Nato as a Military Intelligence Provider

The establishment of the European Union did not affect the organisation of the military defence of its members. The Maastricht Treaty, which declared 'the eventual framing of a common defence policy',[1] explicitly ceded responsibility for security and defence to NATO. This alliance, however, was grappling with the new post-Cold War security environment, and the growing number of issues and challenges affecting not only the United States but also, in close proximity, the countries making up NATO's 'European pillar'. The strategic security problems caused by the disintegration of the Soviet Union and Yugoslavia were translated into political decisions to engage in the enforcement of peace in the Balkans, promote NATO's eastern enlargement in the face of Russia's objections and work out a cooperative formula with the EU.

These 'grand' strategic dilemmas overshadowed new security threats and challenges, such as terrorism, political and religious radicalism, violent extremism and transnational organised crime. Even though NATO's capabilities as developed in the 1990s involved anticipation through high-quality intelligence information and analysis, they were focused on a new military paradigm highlighting intelligence, surveillance and reconnaissance as factors critical to successfully accomplishing missions (Freedman 1998, pp. 52–7; Berkowitz 2003, pp. 19–22; Deptula and Brown 2008; Flynn and Flynn 2012, p. 4; Brown 2014).

Intelligence cooperation in the 1990s was focused on military intelligence sharing during the wars in the Gulf and the Balkans, particularly after NATO took responsibility for peace enforcement (see Cimbala and Forster 2010). The issue of strategic intelligence was subject to needs, capabilities and willingness. All three factors caused trouble, and sometimes confusion, mostly because they revealed strong differences and discrepancies between the EU and NATO. EU intelligence capabilities were at a very early stage of their development, and unanimity as the principal decision-making rule was often subject to national ambitions and prejudices. Mutual trust and confidence in the real intelligence partnership was often undermined by free-riding tendencies or technological, organisational and legal asymmetries (Roberts 2003, pp. 332–8). In a contribution to a research paper on European defence at the end of the 1990s, British analyst Charles Grant bluntly stated that 'Because the EU has a reputation for being a "leaky" organisation, and because some of its members are not-Allied, NATO is reluctant to pass intelligence to the EU' (quoted in Heisbourg 2000, pp. 68–9). EU Member States were aware of these weaknesses and soft regulations concerning access to public documents. Following the political decision at the Helsinki summit in December 1999 to develop military and non-military crisis-management systems within the ESDP framework, the Council decided to adjust EU document protection rules to NATO standards. In 2000 the EU concluded an interim security agreement with NATO, and the Council amended its decision on public access to Council documents (Council of the EU 2000), introducing serious restrictions and practically eliminating the right of access to almost all classified information (Roberts 2003, p. 356).

Strategic disagreements and serious political rows over the Iraqi WMD issue undermined EU–NATO military intelligence cooperation and information sharing for crisis management. Regardless of the emerging 'transatlantic rift' over Iraq, Iran and the global war on terror, the EU pushed hard for the launch of its first ESDP missions. Representatives of the EU Military Committee and the Military Staff were well aware that the planning and preparation of missions and operations require the building of situational awareness and improved intelligence capacities. They were equally aware that NATO's support or direct involvement was indispensable to the initial stage of military action under ESDP. The presumed availability of NATO assets and capabilities, including information sharing and intelligence, was discussed during the final stage of preparation for the first ever military operation commanded by the EU (Simón 2010, p. 15). As this implied a takeover from the NATO-led SFOR, the EU had to work out a package of relevant agreements with NATO, including over information security and intelligence sharing. On 14 March 2003 in Athens, a few days before the US-led 'coalition of the willing' invaded Iraq, NATO and the EU signed an agreement on information security, complemented three months later by provisions on common standards for the protection of classified information (Esterle 2005, p. 51).

The agreement was part of a comprehensive EU–NATO framework for permanent relations. It took the form of a set of cooperation agreements, making up the so-called 'Berlin Plus arrangements' (Matlary 2009, pp. 60–61). The agreement on information security set rules for the exchange of classified information, introducing common safeguards and establishing institutional responsibility for managing the delivery of classified information (European Union 2003). The agreement was supplemented with another document concerning standards for security clearance, registry systems, encryption of electronic transmissions and control over the working of the EU–NATO classified information exchange system (Council of the EU 2003b).

Under the Berlin Plus framework for EU-led military operations, the ALTHEA Operational Headquarters has access to NATO's communication and information systems as well as the intelligence databases (IMPETUS 2009, p. 21). Only two military operations, and as of mid-2015 only one—ALTHEA in Bosnia and Herzegovina—have made use of the information sharing and intelligence support of NATO. In other ESDP/CSDP military operations ('non-Berlin Plus'), formal communication between the EU and NATO was not possible (Kammel and Zyla 2011, pp. 655–6; Tardy 2015, p. 30). The counter-piracy operations around the Horn of Africa conducted by both organisations (NATO's 'Ocean Shield' and EUNAVFOR's 'Atalanta') have evidenced serious limitations, red lines and practical barriers to information exchange and intelligence sharing, regardless of the unity of goals, mission, effort and operational area, according to Gebhard and Smith (2015, pp. 114–17). These authors come to a paradoxical conclusion: 'Two international organizations with 21 coinciding members operating in a common mission area and combating a common threat are kept from sharing intelligence and exchanging information even if it serves shared interests' (Gebhard and Smith 2015, p. 115). So in practice, classified information exchanged among NATO members has not been available to units (vessels) under EU command (Ginsberg and Penksa 2012, p. 222).

One possible solution to this deadlock is an ad hoc agreement between the EU and NATO, allowing for limited information sharing. Another way is a bilateral irregular exchange of information and intelligence. Although the dual membership of the majority of the participating states enables some national-level data and intelligence to be handed over, in practice this is complicated by the total separation of the EU and NATO computer and information infrastructures, the need to declassify shared material and the formal consent of the information originator. Presumably some informal contacts have been maintained, but they are shrouded in great secrecy and consistently denied.[2]

This coinciding yet incompatible membership of the two organisations results in unequal access to classified information. EU Member States which are not members of NATO may not receive NATO classified information. Therefore, 'NATO classified documents or EU classified documents which quote from a NATO classified document, or which describe or paraphrase the content of such document, are not distributed to [these states], unless NATO, as originator of the document, gives its consent to release the information to these Member States' (Council of the EU 2006a).

The transfer of information and intelligence between the two organisations can be both difficult and annoying.[3] The Political and Security

Committee (PSC) is the EU's top institutional link with NATO. Its counterpart, the North Atlantic Council (NAC), operates at a high political level predetermined by the Member States' elaborated positions. Since the NAC is chaired by the Secretary General and the PSC by the HR/VP, the NAC and PSC meetings are a good opportunity for the direct exchange of formal and informal communications, including those of a sensitive security nature.[4] Both top officials are also invited to the ministerial meetings of the respective partner organisations and thereby kept informed about the major topics on the table (Duke 2005, p. 16; Smith 2013b, p. 49). Within the military structures, NATO set up the Permanent Liaison Team to the EUMS in 2005, and an EU cell was established at SHAPE (NATO's Supreme Headquarters Allied Powers Europe) (Norheim-Martinsen 2010, p. 8), both designed for active collaboration in operational settings.

The EU's supply of strategic intelligence from NATO is severely limited. This is especially relevant to effective cooperation on new security threats, such as terrorism, cyber-threats or radicalisation. Both organisations have reaffirmed their willingness to develop closer cooperation on combating terrorism, including the exchange of information on relevant subjects (Santamato and Beumler 2015, pp. 41–3), but they have yet to establish a permanent CIS arrangement allowing for the effective and systematic mutual delivery of relevant information on new threats and challenges. Strategic intelligence cooperation between NATO and the EU is also limited by the general value of shared products. Deficits in reliable communication infrastructure, political will and national safeguards mean that rather than original intelligence being generated from raw information provided by national intelligence services, finished intelligence is generated from pre-processed and analysed information held by Member States (Clarke and McCaffrey 2004, p. 16).

Deficiencies and shortcomings of intelligence support at the strategic level, as well as certain problems in operating communication and information systems, effectively hamper intelligence sharing. Although direct secure links are activated between operational headquarters, they are often established on an ad hoc basis and serve mainly operational tasks (Simón 2010, p. 41). The critical factor is the stance and policy of the United States as leader of the NATO alliance. US scepticism about sharing sensitive NATO information and intelligence with EU institutions limits mutual cooperation. However, the USA has developed effective cooperation arrangements with the EU on non-military aspects of security.

The United States: An Assertive Ally

Cooperation between the USA and its European allies has always been a sensitive and, consequently, secretive topic. The beginnings of this collaboration can be traced back to the late 1960s, when the growing wave of Arab terrorism encouraged the United States and its European partners as well as Israel to cooperate in exchanging information about the most dangerous Palestinian activists. At the beginning of the 1970s, anti-terrorism officials from EEC Member States held a series of consultations on internal security and possible measures against predominantly external threats (Bunyan 1993, p. 16). The United States were invited to those secret consultations under the framework of the Berne Club as late as 1971 (Bigo 1992a, p. 145). The Trevi Group, an informal, secret 1976 initiative by interior ministers of EC Member States attracted the attention of a US administration eager to participate in information exchange on prominent security issues. The USA then set up informal contacts with Trevi officials as one of the 'Friends of Trevi' countries, along with Sweden, Austria, Switzerland and Canada, among others (Bunyan 1993, p. 16; den Boer 1998, p. 109). In 1979 the United States launched another antiterrorist initiative, focusing on Palestinian and Armenian radicals operating in Western Europe and North America. A working group called the Quantico Club was formed as a joint effort by the USA, Canada, West Germany, the UK, France, Sweden and Australia (Bigo 1992b, p. 51; Monet 1993, p. 314). These secret anti-terrorist efforts proved important in dealing with the manifestations of leftist radicalism, Palestinian extremism and state-sponsored terrorism, mainly of Libyan provenance, that were taking place in Western Europe and affecting US strategic interests.

Facing new challenges and threats to their security resulting from growing instability in the Middle East and Southern Asia, as well as the upheaval in Eastern Europe, representatives of the United States, the EEC and its Member States adopted the joint declaration 'Transatlantic Challenges' in November 1990,[5] underlining their 'responsibility to address transnational challenges', such as preventing and combating terrorism, putting an end to illegal drug production and trafficking, and cooperating in the fight against international crime. In practical terms, however, Euro-Atlantic cooperation was developing at a slow pace, lacking political momentum and an organisational basis (Rees 2011, pp. 398–9). With the creation of the European Union, the US administration showed more interest in reinforcing transatlantic cooperation. On 3 December 1995 at the

EU–US summit in Madrid, the New Transatlantic Agenda (NTA) was signed (Rees 2006, pp. 41–2). The declaration contained a modest statement on the shared desire to 'cooperate on assessing and responding to terrorist threats'.[6] More specific and detailed provisions on further cooperation in preventing and fighting principal threats to security were contained in a joint EU–US action plan. On information exchange, it declared a commitment to further cooperation on assessing and responding to terrorist threats. It signalled the mutual desire to share information and analyses of emerging trends in international criminal activity, especially sensitive information on the production of illegal drugs. It also looked forward to concluding an agreement on cooperation between Europol and the US administration as soon as Europol commenced its full activities.[7]

These plans were given a strong boost in the aftermath of the terrorist attacks on the United States on 11 September 2001 (Hamilton 2003, pp. 552–4; Daalgard-Nielsen 2004; Rees 2011, pp. 398–400). Heads of state and government as well as JHA ministers from EU Member States declared their readiness for increased cooperation in combating terrorism in every form. While ministers and heads of governments were debating anti-terrorist activities, an EU delegation, with High Representative Javier Solana at its head, held a series of meetings in Washington with senior White House officials, among them US Secretary of State Colin Powell and the National Security Advisor Condoleezza Rice (Rees 2006, pp. 79–80; EU Observer 2001a). At the end of the talks they declared that 'the US and the EU will vigorously pursue cooperation in a number of security fields, including police and judicial cooperation, border controls, visa and document security issues as well as law enforcement access to information and exchange of electronic data' (White House 2001). Cooperation between Europol and the US authorities was discussed and ended in a formal agreement signed on 6 December 2001. It provided for the exchange of strategic and technical information on serious crime and terrorism between Europol and the United States, but it did not authorise the transmission of data related to individuals (EU Observer 2001b; Lindstrom 2003, p. 249). In the following months a series of other measures were discussed, including: the drawing up of lists of terrorist individuals and organisations and the freezing of their assets; developing judicial cooperation in criminal matters, including mutual legal assistance and extradition; combating terrorist financing; exchanging information held by law-enforcement and judicial authorities; and exchanging personal data and related information on the basis of the 2001 Europol–US agreement (Mitsilegas 2003, p. 520; Georgopoulos 2005, pp. 198–9). Close contact was further strengthened in November 2005 when the United States Secret Service signed a cooperation agreement with Europol providing for improved information sharing and the exchange of personal data related to transnational organised crime (NIEUWS Bank 2005).

The scope of cooperation and intensity of contacts between US officials and representatives of relevant EU institutions and agencies suggested the emergence of a system of 'transatlantic homeland security' (Lindstrom 2006, pp. 115–17; Borchert 2006, pp. 4–5; Pawlak 2009, 2010a). Multilateral cooperation coincided with the strengthening of hitherto working alliances with long-standing European partners, such as the UK, Germany and Italy, or rebuilding close operational contacts with competitors, namely France. After 9/11 the UK and USA strengthened their 'special relationship' with well grounded and structured bi- and multilateral connections (Johnston 2005b, pp. 46–7; Svendsen 2008a; Dumbrell 2009). As Adam Svendsen (2010, p. 3) points out, 'despite some asymmetry, the UK–US intelligence relationship is arguably one of the "best" examples of an effective international intelligence liaison relationship'. The bilateral UK–USA agreement and joint participation in multilateral arrangements such as 'Five Eyes' (SIGINT and electronic surveillance) or the SAG Group (international criminal issues) consolidated the ties between the two partners (Richelson and Ball 1985; Stafford and Jeffreys-Jones 2000).

US relations with Germany, robust during the Cold War (Krieger 2011), also proved useful in the post-9/11 conditions of uncertainty (Naftali 2004). Former German Ambassador to the USA Wolfgang Ischinger (2004, pp. 22–30) underlined the intensification of counter-terrorism cooperation with the USA after 9/11. Irrespective of the political dispute over military intervention in Iraq, US and German intelligence services collaborated closely in numerous fields, including joint SIGINT activities, based on the 2002 NSA-BND memorandum of agreement (Spiegel 2014), intelligence sharing on Iraq, WMD counter-proliferation or the container security initiative (Miko and Froehlich 2004). Later, intelligence exchange went even further, encompassing access to biometric data and the spontaneous sharing of data about known and suspected terrorists (BTT 2008, pp. 3–4).

France, despite her different views on the US role in European security and political cooperation, followed the example of her big EU counterparts. After 9/11 the French intelligence services fully cooperated with their US partners in seeking out al Qaeda's network and those of other radical Islamist organisations in Europe and worldwide (Pauly 2005, pp. 7, 11). In May 2002, the CIA and the French Direction Générale de la Sécurité Extérieure (DGSE) launched a secret operation code-named 'Camolin' (LCI 2005). In February 2003 they established headquarters in a Paris military barrack, hosting regular top-secret meetings of intelligence officials from the USA, France, Germany, the UK, Canada and Australia, in an informal network called the 'Alliance Base' (*Le Monde* 2006). Its main objectives included the analysis and tracking of the transnational movements of terrorist suspects (Aldrich 2009, pp. 130–1). The best-known result of the Alliance Base cooperation was the apprehension of Christian Ganczarski, al Qaeda's 'German general' (Vermaat 2007; Trifunovic 2014, pp. 32–3). John E. McLaughlin, former director of the CIA, claimed that the relationship between the French DGSE and the CIA 'is one of the best in the world' (Aldrich 2009, p. 131).

Political tensions over military intervention in Iraq and contrasting threat perceptions (Rees 2006, pp. 69–78) limited progress in information sharing and intelligence cooperation. However, in the aftermath of the terrorist attack on Madrid in 2004, the United States and EU Member States adopted the Declaration on Combating Terrorism (Council of the EU 2004a). They renewed their commitment to further developing cooperation against terrorism within the framework of the New Transatlantic Agenda. They declared their intention to improve cooperation on the sharing of law-enforcement and other sensitive information, and to strengthen the capacity for cooperation between the USA and Europol. Nevertheless, observers noted deadlocks in counter-terrorism strategy areas relevant to the USA, such as cooperation with the EU in passenger name record (PNR) exchange, mutual legal assistance in criminal matters, and combating terrorist financing. Disappointed, the Bush administration sought additional ways to revive mutual collaboration in the framework of the transatlantic dialogue on combating international terrorism. It approached the G6 group and since May 2007 the US Secretary of Homeland Security and Attorney General have attended its ministerial meetings.

The USA also sought to strengthen its arguments regarding law-enforcement data sharing and judicial cooperation in criminal matters (Statewatch 2009). In April 2007 an EU–US agreement on the security of classified information was concluded, setting out the terms of protection of mutually exchanged classified information (European Union 2007). Landmark decisions taken by the European Parliament and the Council at the beginning of the 2010s with respect to the US–EU agreements on extradition and mutual legal assistance, on personal data exchange and on terrorist financing put an end to low-profile intelligence cooperation (Fahey 2014, pp. 147–9).

The US-driven 'need-to-know' principle which underpinned transatlantic intelligence cooperation after 9/11 was consistently applied in ever-widening fields of counter-terrorism policy. It also covered civil aviation and access to information about passengers on foreign flights to or from the United States (Salter 2010). In 2001 the US Congress adopted the Aviation and Transportation Security Act (ATSA), requiring all airlines arriving in or departing from the USA to provide their passenger data to US Customs for the purpose of combating terrorism and other serious criminal offences. The ATSA provisions were subsequently extended, requiring airlines to grant access to PNR data. For EU institutions mandated with protection of privacy (the European Parliament, the Council's Article 29 Working Party on Data Protection, the European Data Protection Supervisor), this US legislation raised serious legal doubts and technical queries. It contravened EU data protection rules, especially the 1995 EC Data Protection Directive (95/46/EC) which explicitly prohibited any processing of sensitive personal data without specific authorisation (Pawlak 2010b, pp. 117–18). For the Council and the Commission, however, cooperation with US authorities in preventing and countering global terrorism was the priority and PNR transmission to proper US agencies was considered to be indispensable regardless of legal reservations (den Boer 2011, pp. 346–8; Zaiotti 2012, pp. 331–2).

As a result, in February 2003 the European Commission agreed a deal with the US customs authorities on the granting of online access to PNR by European airlines to US authorities, while searching for a mutually satisfactory solution (Adam 2006, pp. 663–5; Argomaniz 2009b). Authorised by the Council, in February 2004 the Commission began negotiations on the processing and transfer of airlines' PNR data to the US Department of Homeland Security. The agreement was quickly concluded and in May 2004 the Council approved it (Council of the EU 2004b). The European Parliament, however, contested the lack of strict data-protection safeguards and launched proceedings before the Court of Justice of the EC (ECJ) to annul both the PNR agreement and the respective Council decision. In May 2006, the ECJ issued a judgment declaring the EU–US PNR agreement unlawful. US and European negotiators concluded another agreement, providing expanded US access to

PNR data collected by airlines: it allowed the Department of Homeland Security to share PNR data with other US agencies engaged in the fight against terrorism, extending the length of time that the USA can store such data and allowing it to access sensitive information about a passenger (De Hert and De Schutter 2008, pp. 325–6; Papakonstantinou and De Hert 2009, pp. 903–7). Once again, the European Parliament raised numerous concerns over the text of the new agreement and, following a lengthy discussion, demanded the opening of new PNR negotiations with the United States. The new bilateral agreement between the EU and the US was signed in December 2011 and several months later approved by the European Parliament (Murphy 2012, pp. 159–62).

The 2011 EU–US PNR agreement entitles competent US authorities to collect, use and process PNR for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and related crimes as well as other transnational crimes punishable by a minimum prison sentence of three years. To the extent that a PNR includes sensitive data, the US Department for Homeland Security should employ automated systems to filter out and mask such data. However, access to, as well as the processing and use of, sensitive data is permitted in exceptional circumstances where the life of an individual could be imperilled or seriously impaired. In such cases sensitive data may be retained for the time specified in US law for the purpose of a specific investigation, prosecution or enforcement action.

Another important EU–US counter-terrorism arrangement involving information sharing was an agreement on the use of banking data to tackle the issue of the financing of terrorism. One of the first instruments launched by the USA in the aftermath of the 9/11 attacks was the secret Terrorist Finance Tracking Program (TFTP). This aimed to track terrorists and their networks in order to trace sources of the financing of their activities worldwide (Murphy 2012, pp. 151–2). The TFTP used certain kinds of financial transaction information, including the personal data of bank customers, provided by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a Belgium-based global financial messaging service which facilitates international money transfers. After 9/11, SWIFT complied with US Department of the Treasury demands that SWIFT should provide access to information held in the United States (Kierkegaard 2011, pp. 452–3; De Goede 2012, pp. 216–17).

After media disclosure of the TFTP's existence in mid-2006, the European Parliament passed a resolution (European Parliament 2006) strongly disapproving 'any secret operations on EU territory' affecting the privacy of EU citizens and expressed serious concerns as to the purposes of the transfer of data to the US Treasury Department. It urged the United States and its intelligence and security services to act in a spirit of good cooperation and notify their allies of any security operations they intend to carry out on EU territory. Following privacy concerns (Ripoll Servent and Mackenzie 2012; SWIFT 2012), representatives of the US administration and the EU began negotiations in 2009 on an agreement allowing the use of banking data in anti-terrorist investigations. An interim agreement allowed US authorities continuous access to SWIFT information flows. This was questioned by several EU Member States and rejected by the European Parliament (Monar 2010, p. 143; Suda 2013, pp. 772–3). A new agreement was signed in June 2010 and was approved by the European Parliament the following month (Pop 2010). Although the US administration had to arrive at a compromise with the EU on data-protection safeguards and supervisory mechanisms, the agreement concluded set out binding principles for all specific transfer agreements aimed at tracking terrorist financing. Therefore, the transfer or processing of personal data could be permitted for explicit purposes in the framework of the fight against terrorism.

The adoption of these arrangements did not dispel doubts over the proper mechanisms for securing personal data exchanged across the Atlantic. In November 2010 the Council, on the recommendation of the European Commission, adopted negotiating directives for a framework agreement (the so-called 'Data Protection Umbrella Agreement') on the protection of personal data transferred between the EU and the USA for law-enforcement purposes, especially for the prevention, detection, investigation and prosecution of criminal offences, including terrorism (Council of the EU 2010g, p. 7). The negotiations started formally in March 2011 but, despite two dozen rounds having already been conducted, they have advanced slowly and achieved little. The reasons can be found mostly in the political and normative domains seriously affected by the so-called Snowden affair (Greenwald 2014; Harding 2014; Gurnow 2014; Goldfarb 2015). The disclosure in June 2013 by former NSA contractor Edward Snowden of the scope of the surveillance conducted by US intelligence agencies in Europe caused profound unease in government circles in key allies of the US in the European Union, most of all in Germany. Revelations about the mass interception of secret communications between European political leaders, and even the wiretapping of high-ranking EU officials had a negative impact on official EU–US relations, including the talks on the Umbrella Agreement.

If some initial progress had been made, as declared in the joint EU–US statement in June 2012, the Snowden affair sharpened differences concerning the terms of access by government authorities to private data in the fight against organised crime or terrorism and the issue of data-retention periods, where data is ued for purposes other than criminal investigations (Bendiek 2014, p. 5). Although the stalemate was overcome, and even seemed to gain fresh impetus from the March 2014 EU–US summit (Council of the EU 2014e), a critical outstanding issue has yet to be finally settled. US foreign intelligence gathering, both inside and outside the United States, follows a two-track system: one for US persons and another for non-US persons (Bignami 2015, p. 29). This affects the right of judicial redress as a remedy for data protection violations. It should ensure that EU citizens not resident in the United States are granted the same rights as those enjoyed by US nationals in the EU. Although the Umbrella Agreement would not be decisive for information sharing in law enforcement as a whole, it should nevertheless facilitate further existing formally established cooperation.

The External Dimension of the Criminal Intelligence Hub

Cooperation with actors located outside the transatlantic security community has been rather limited and has focused on terrorism, information sharing, criminal intelligence and risk analyses at external borders. It involves dedicated EU agencies, namely Europol, Eurojust and Frontex, authorised to conclude agreements on information exchange. They use established mechanisms, instruments and modes of information exchange to produce strategic and analytical reports and assessments.

Europol has 14 operational agreements and seven strategic agreements with countries and organisations around the world, including the International Criminal Police Organisation, Interpol. The partner countries are European neighbours, North American strategic partners and a country with a specific position on the global map of criminality: Colombia. Moreover, the Council recommended to Europol that it negotiate agreements with four states: Brazil, Mexico, Georgia and the United Arab Emirates. The partners must ensure an adequate level of data protection to comply with EU standards (Boehm 2012, pp. 209–10). The content of these agreements is substantially focused on the exchange of information and broad analytical materials, including strategic analyses, situational reports and threat assessments. Obviously, operational agreements define the terms of cooperation more precisely with regard to data security and classification, usage and dissemination, personal data safeguards, and liability. Strategic agreements are more general, and refer mainly to categories of information, procedures of information exchange, and confidentiality rules. Moreover, the strategic and operational agreements differ as regards personal data exchange. Strategic agreements do not allow for the exchange of personal data although an opportunity to conclude a relevant separate agreement is taken into account.

The exchange of information and analytical material takes place between established national contact points in the partner country and Europol. Every partner country may establish a liaison office at Europol Headquarters to facilitate information exchange and cooperation with Europol. If required, Europol may also establish a liaison office in the partner country. Information is transmitted via secure communication channels. It is subject to a basic level of security unless any of the partners marks the information with an elevated security level. In some cases, however (e.g. Ukraine, Colombia), restricted and secret information may not be either wholly or partially transmitted electronically but is dispatched by traditional messenger. Personal data is additionally protected according to the binding national legislation of the partner country. Information supplied by external partners goes to Europol's 24/7 operational centre where it is processed, ensuring that data received from a third country is assessed for authenticity and accuracy before being forwarded to a dedicated database or analytical file at Europol, which may also check the competence of the originator as well as the reliability of the source. The majority of third countries can use the SIENA secure application. Other partners contact the operational centre through national points of contact or liaison officers. The centre is also responsible for timely and accurate responses to requests for information or analysis from third countries. Although only about 4 per cent of the data in cases initiated in 2014 came from external partners (Europol 2015b), Europol retains the profitable option of requesting information for analytical as well as operational purposes. Cooperation with Interpol facilitates access to criminal information concerning other third countries and also supplementary information on Europol's partner states.

Frontex has concluded working arrangements with 17 countries in Europe, Asia, Africa and North America and two regional centres (in the Commonwealth of Independent States and in the Western Balkans).

Since these arrangements do not have the status of international treaties, their implementation remains optional. A single cooperation agreement between Frontex and non-EU states and organisations is not possible due to differences of location, borders and migratory movements, so these working arrangements differ markedly in terms of information exchange, intelligence sharing, communication systems and general terms of availability. The arrangements—with the exception of the Russian Federation—allow for the exchange of information and analytical products which in most cases are unclassified. Some countries, (e.g. Armenia, Azerbaijan, Nigeria) can exchange classified information or intelligence subject to a separate security agreement or protocol. Partner countries with greater data protection and privacy restrictions (Canada, the United States) are not authorised or required to transmit personal information or data related to an identified individual. Frontex may provide relevant analytical products. However, access to tailored risk analysis and respective information is decided by the Executive Director on a case-by-case basis.

Communication is maintained by the established contact points (usually the border guards or immigration services of the partner countries). Agreements with some countries (e.g. Cape Verde, Montenegro, Albania) allow a national risk-analysis expert to participate as an observer in relevant meetings of the Frontex Risk Analysis Network. The external information network established by Frontex is potentially profitable for the agency's analytical capacities and situational awareness building. Frontex has access to substantial information resources and analytical products held by the majority of the partners. It may also consult relevant border services on an ad hoc or regular basis. However, although these working arrangements are politically binding they have soft legal grounds. It is entirely up to the counterparts to decide the extent of their cooperation and the categories of data, information and analysis they are willing to share. Moreover, without a standard electronic communication connection, there is little scope for the exchange of sensitive information.

The third EU JHA agency, Eurojust, has maintained cooperation with a relatively smaller group of non-EU countries. Agreements were concluded with the EEA members incorporated into the Schengen zone and participating actively in the EU area of freedom, security and justice: Switzerland, Norway, Iceland and Liechtenstein. Macedonia (FYROM) and Moldova signed agreements due to the high level of criminality originating in these countries and affecting EU Member States. There are also agreements with Interpol and the UN Office on Drugs and Crime.

Eurojust exchanges mainly operational information on ongoing investigations in transnational cases. Some information can be used, nevertheless, for strategic criminal analysis within the framework of the ECIM or under specific inter-institutional arrangements with other EU agencies, mainly Europol.

Concluding Remarks

The extension of cooperative intelligence links outside the EU and its Member States has been motivated by the following factors:

- the globalisation of threats and challenges to EU security, requiring its intelligence structures to extend their reach;
- shortcomings and limitations of military intelligence capabilities in the EU;
- low trust and problematic credibility of some Member States, requiring external compensatory measures;
- capability gaps in such areas as human intelligence or satellite imagery.

Additionally, the major EU members, such as the UK, Germany and France, have developed close relationships with their external partners, either on a bilateral basis or in multilateral settings.

While the external military dimension of EU security relies greatly on the NATO alliance, internal security policy has become a wider and more diversified field, open to various forms of collaboration with different external partners ranging from close neighbours (the Eastern Partnership, the Union for the Mediterranean) and strategic partners (the USA) to regional blocs (the Africa-Frontex Intelligence Community) and remote partners (Australia) (Hobbing 2010). Since the sharing of military intelligence has been subject to numerous restrictions, it has usually occurred on a case-by-case basis. Criminal intelligence cooperation with external partners has addressed global risks and threats generated by organised criminality, illicit cross-border activities and cybercrime. Using large-scale information management and knowledge assessment, it has sought to acquire additional input from selected countries and organisations willing to respond positively to the EU's 'need-to-know' principle.

External intelligence cooperation has focused on the United States. After 9/11 the US administration actively sought to widen the scope of its partnership with EU Member States in the area of security and counter-terrorism, and especially to go beyond the EU's institutional and legal framework, substituting state-to-state activity for formal EU–US initiatives caught in a procedural stalemate, and pressing its EU allies to proceed with jointly agreed undertakings at EU institution level. The G6–US cooperation has provided good examples of such arrangements (Bossong 2007).

For the European Union and its institutions the concept of information exchange within the framework of 'transatlantic homeland security' was rather controversial (Cox 2005, p. 223). No common vision of homeland security existed across the Union and the approach to threats and challenges was reactive and gradual (Lindley-French 2002, pp. 36–7)—hence the tortuous process of adopting EU–US agreements on US access to airline passenger data. As the European Commission (2010a, p. 4) admitted, 'PNR are mainly used as a criminal intelligence tool'. They can be used both preventively and proactively, focusing on the identification of individuals, risk assessment and—in exceptional circumstances—criminal/terrorist profiling. The PNR agreement actually served both criminal intelligence and anti-terrorist objectives, which was also true of the 2005 EU–Canada PNR agreement (Hobbing 2010).

The complex decentralised structure of intelligence cooperation in the EU has enabled the gradual emergence of a wide and complex network of communication and information-sharing services which vary widely. Most commonly, EU agencies and units are granted access to certain information or acquire intelligence products on request. However, this is too often done on a case-by-case basis or relies on ad hoc decisions rather than established systems. A notable exception is transatlantic intelligence cooperation (Clarke 2004, pp. 129–30). According to one expert, this remains a complex network 'with few key nodes or hierarchies and not a little duplication' (Aldrich 2009, p. 128).

The European Union, pursuing its security strategy in a globalised environment, has sought to extend its intelligence security structures far beyond the territory of Member States. An efficient, mutually beneficial and politically acceptable exchange of sensitive data and intelligence has not always been possible. The EU intelligence community has failed to take advantage of all possible solutions, available instruments and potential capabilities. Nonetheless, it has managed to establish flexible network arrangements with external partners that contribute to enhanced intelligence security capabilities.

Notes

1. Article J.4.1. of the Treaty on the European Union signed at Maastricht on 7 February 1992 (European Union 1992).
2. Anonymous NATO official, interview, June 2012; anonymous EEAS official, interview, June 2012.
3. Anonymous NATO official, interview, June 2012; anonymous EEAS official, interview, November 2012.
4. Anonymous EEAS official, interview, June 2012; anonymous NATO official, interview, June 2012).
5. The text was published in Barbour (1996, pp. 99–101). See also Cullen (1998, p. 84).
6. The text is available at EEAS (2015a).
7. The text is available at EEAS (2015b).

Bibliography

Adam, S. (2006). Quelques réflexions sur les relations entre les procédures a priori et a posteriori d'examen de compatibilité des accords communautaires suite à l'affaire dite de l'«accord PNR». *Cahiers de droit européen, 5*(6), 657–696.

Aldrich, R. J. (2009). US–European intelligence co-operation on counter-terrorism: Low politics and compulsion. *British Journal of Politics and Intenational Relations, 11*(1), 122–139.

Argomaniz, J. (2009b). When the EU is the 'norm-taker': The passenger name records agreement and the EU's internalization of US border security norms. *European Integration, 31*(1), 119–136.

Barbour, P. (Ed.). (1996). *The European Union handbook*. Chicago/London: Fitzroy-Dearborn Publishers.

Bendiek, A. (2014). *Tests of partnership transatlantic cooperation in cyber security, internet governance, and data protection*. SWP Research Paper RP. Berlin: Stiftung Wissenschaft und Politik.

Berkowitz, B. (2003). *The new face of war. How war will be fought in the 21st century*. New York: The Free Press.

Bignami, F. (2015). *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens*. Brussels: European Parliament.

Bigo, D. (Ed.). (1992a). *L'Europe des polices et de la sécurité intérieure*. Paris: Editions Complexe.

Bigo, D. (1992b). L'Europe de la sécurité intérieure. In D. Bigo (Ed.), *L'Europe des polices et de la sécurité intérieure*. Paris: Editions Complexe.

Boehm, F. (2012). *Information sharing and data protection in the area of freedom, security and justice. Towards harmonised data protection principles for information exchange at EU-level.*. Berlin/Heidelberg: Springer-Verlag.

Borchert, H. (2006). Homeland security and transformation: Why it is essential to bring together both agendas. In E. Brimmer (Ed.), *Transforming homeland security: U.S. and European approaches*. Washington, DC: Center for Transatlantic Relations.

Bossong, R. (2007). *The European security Vanguard? Prüm, Heiligendamm and flexible integration theory*. LSE/Challenge Working Paper. At http://www.libertysecurity.org/article2160.html. Accessed 24 Apr 2007.

Brown, J. M. (2014). Strategy for intelligence, surveillance, and reconnaissance. *Joint Force Quarterly, 72*, 39–46.

BTT. (2008). US and Germany to share terrorist fingerprint data. *Biometric Technology Today, 16*(4), 3–4.

Bunyan, T. (Ed.). (1993). *Statewatching the new Europe. A handbook on the European state*. Radford Mill: Russell Press for Statewatch.

Cimbala, S. J., & Forster, P. K. (2010). *Multinational military intervention: NATO policy, strategy, and burden sharing*. Farnham/Burlington: Ashgate.

Clarke, J. (2004). The United States, Europe, and homeland security: Seeing soft security concerns through a counterterrorist lens. *European Security, 13*(1), 117–138.

Clarke, R. A., & McCaffrey, B. R. (2004). *NATO's role in confronting international terrorism*. Washington, DC: Atlantic Council of the United States.

Council of the EU (2000, August 23). Council decision of 14 August 2000 amending decision 93/731/EC on public access to council documents and council decision 2000/23/EC on the improvement of information on the council's legislative activities and the public register of council documents. *Official Journal of the European Communities, L 212*.

Council of the EU (2003b, June 3). Security standards between the NATO Office of Security (NOS), the EU Council General Secretariat Security Office (GSCSO) and the European Commission Security Office (ECSO) for the protection of classified information exchanged between NATO and the EU, annex to document 10006/03, Brussels.

Council of the EU (2004a, June 26). EU-U.S. declaration on combating terrorism. Dromoland Castle, 26 June 2004, doc. 10760/04, Dromoland Castle.

Council of the EU (2004b, May 20). Council Decision of 17 May 2004 on the conclusion of an agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (2004/496/EC). *Official Journal of the European Union, L 183*.

Council of the EU (2006a). Guide on the security of information: September 2006. At http://bookshop.europa.eu/en/guide-on-the-security-of-information.-september-2006-pbQCX106131/downloads/QC-X1-06-131-EN-C/QCX106131ENC_001.pdf. Accessed 12 Oct 2013.

Council of the EU (2010h, March 3). Council decision of 25 February 2010 on setting up the Standing Committee on operational cooperation on internal security. *Official Journal of the European Union, L 52.*

Council of the EU (2014e, March 26). EU-US summit joint statement, 8228/14, Brussels.

Cox, M. (2005). Beyond the west: Terrors in Transatlantia. *European Journal of International Relations, 11*(2), 203–233.

Cullen, D. (1998). Transatlantic relations in the field of justice and home affairs—Can the EU really deliver? In J. Monar (Ed.), *The new transatlantic agenda and the future of EU-US relations*. London/The Hague/Boston: Kluwer Law International.

Dalgaard-Nielsen, A. (2004). Homeland security. American and European responses to September 11th. In J. Pilegaard (Ed.), *The politics of European security*. Danish Institute for International Studies: Copenhagen.

De Hert, P. J. A., & De Schutter, B. (2008). International transfers of data in the field of JHA: The lessons of Europol, PNR and SWIFT. In S. Thiel & B. Martenczuk (Eds.), *Justice, liberty, security: New challenges for EU external relations*. Brussels: VUB Press.

De Goede, M. (2012). The SWIFT affair and the global politics of European Security. *Journal of Common Market Studies, 50*(2), 214–230.

Den Boer, M. (1998). Defying a global challenge: Reflections about a joint EU-US venture against transnational organized crime. In J. Monar (Ed.), *The new transatlantic agenda and the future of EU-US relations*. London/The Hague/Boston: Kluwer Law International.

Den Boer, M. (2011). Soft, smart and strategic. The international dimension of EU action in the fight against terrorism. In M. Cremona, J. Monar, & S. Poli (Eds.), *The external dimension of the European Union's area of freedom, security and justice*. Brussels: P.I.E. Peter Lang.

Deptula, D. A., & Brown, R. G. (2008). A house divided: The indivisibility of intelligence, surveillance, and reconnaissance. *Air & Space Power Journal, 22*(2). At www.airpower.au.af.mil/airchronicles/apj/apj08/sum08/deptula.html. Accessed 11 Aug 2012.

Duke, S. (2005). *The Linchpin COPS: Assessing the workings and institutional relations of the Political and Security Committee*. Working Paper 2005/W/05. Maastricht: EIPA.

Dumbrell, J. (2009). The US–UK special relationship: Taking the 21st-century temperature. *British Journal of Politics and International Relations, 11*(1), 68–75.

Esterle, A. (2005). National and European information security policies. In B. Schmitt (Ed.), *Information security: A new challenge for the EU*. Chaillot Paper No. 76. Paris: EU Institute for Security Studies.

EU Observer (2001a, September 19). EU-US meeting to focus on anti-terrorism. *EU Observer*. At https://euobserver.com/news/3508. Accessed 20 Sept 2001.

EU Observer (2001b, December 7). Europol-US accord excludes personal data exchange. *EU Observer*. At https://euobserver.com/news/4467. Accessed 9 Dec 2001.

European Commission (2010a, September 21). Communication from the commission on the global approach to transfers of passenger name record (PNR) data to third countries, doc. COM(2010) 492 final, Brussels.

European Parliament (2006). Resolution on the interception of bank transfer data from the SWIFT system by the US secret services (P6_TA-PROV(2006)0317). At http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/res_060706/res_060706en.pdf. Accessed 26 June 2012.

European Union (1992, July 29). Treaty on the European Union signed at Maastricht on 7 February 1992. *Official Journal of the European Communities, C 191*.

European Union (2003). Agreement between the European Union and the North Atlantic Treaty Organisation on the security of information. *Official Journal of the European Union*, L 80, 27 March.

European Union (2007). Agreement between the European Union and the government of the United States of America on the security of classified information. *Official Journal of the European Union*, L 115, 3 May.

Europol (2015b). SIENA At https://www.europol.europa.eu/content/page/siena-1849. Accessed 14 Mar 2015.

Fahey, E. (2014). Towards a transatlantic community of law? The use of law between the EU and US legal orders: Questions of legal form and characterisation. In E. Fahey & D. Curtin (Eds.), *A transatlantic community of law: Legal perspectives on the relationship between the EU and US legal orders*. Cambridge: Cambridge University Press.

Flynn, M. T., & Flynn, Ch. A. (2012). Integrating intelligence and information: Ten points for the commander. *Military Review, XCII*(1), 4–8.

Freedman, L. (1998). The revolution in strategic affairs. *Adelphi Paper, 38*(318), 5–10.

Gebhard, C., & Smith, S. J. (2015). The two faces of EU–NATO cooperation: Counter-piracy operations off the Somali coast. *Cooperation and Conflict, 50*(1), 107–127.

Georgopoulos, T. (2005). What kind of treaty making power for the EU? Constitutional problems related to the conclusion of the EU-US agreements on extradition and mutual legal assistance. *European Law Review, 30*(2), 198–199.

Ginsberg, R. H., & Penksa, S. A. (2012). *The European Union in global security. The politics of impact*. Basingstoke/New York: Palgrave Macmillan.

Goldfarb, R. (Ed.). (2015). *After Snowden. Privacy, secrecy, and security in the information age*. New York: St. Martin's Press.

Greenwald, G. (2014). *No place to hide. Edward Snowden, the NSA and the surveillance state*. London: Penguin Books.

Gurnow, M. (2014). *The Edward Snowden affair. Exposing the politics and media behind the NSA Scandal*. Indianapolis: Blue River Press.

Hamilton, D. (2003). Three strategic challenges for a global transatlantic partnership. *European Foreign Affairs Review, 8*(4), 543–555.

Harding, L. (2014). *The Snowden files. The inside story of the world's most wanted man*. New York: Vintage Books.

Heisbourg, F. (2000). *European defence: Making it work*. Chaillot Paper no. 42. Paris: Institute for Security Studies of WEU.

Hobbing, P. (2010). Tracing terrorists. The European Union–Canada agreement on passenger name record (PNR) matters. In M. B. Salter (Ed.), *Mapping transatlantic security relations. The EU, Canada, and the war on terror*. London/New York: Routledge.

IMPETUS (2009). EUFOR ALTHEA. Successful contribution to stabilisation. *Impetus. Bulletin of the EU Military Staff, 7*, 21–23.

Ischinger, W. (2004). Fighting Terrorism – International Cooperation as a Strategy of Prevention. *IHS Journal of Homeland Security*, April, 22–30.

Johnston, M.T. (2005b). Britain and Transatlantic Security: Negotiating Two Bridges Far Apart. In T. Lansford & B. Tashev (Eds.), *Old Europe, new Europe and the US: renegotiating transatlantic security in the post 9/11 era*. Aldershot/Burlington: Ashgate.

Kammel, A., & Zyla, B. (2011). Looking for a 'Berlin-Plus in reverse'? NATO in search of a new strategic concept. *Orbis, 55*(4), 648–661.

Kierkegaard, S. (2011). US war on terror EU SWIFT(ly) signs blank cheque on EU data. *Computer Law & Security Review, 27*(5), 451–464.

Koutrakos, P. (2015). *EU international relations law* (2nd ed.). London: Bloomsbury.

Krieger, W. (2011). German–American intelligence relations, 1945–1956: New evidence on the origins of the BND. *Diplomacy and Statecraft, 22*(1), 28–43.

LCI (2005, July 4). Antiterrorisme—Nom de code: Alliance Base. *LCI.fr*. At http://tf1.lci.fr/infos/france/2005/0,,3229765,00-nom-code-alliance-base-.html. Accessed 2 Sept 2008.

Le Monde (2006, September 13). La France abrite une cellule antiterroriste secrète en plein Paris. *Le Monde*. At http://www.lemonde.fr/web/article/0,1-0@2-3224,36-812394@51-812238,0.html. Accessed 15 Sept 2006.

Lindley-French, J. (2002). *Terms of engagement. The paradox of American power and the transatlantic dilemma post-11 September*. Chaillot Paper no. 52. Paris: EU Institute for Security Studies.

Lindstrom, G. (2003). Terrorism: European myths and realities. In G. Lindstrom (Ed.), *Shift or rift. Assessing EU-US relations after Iraq*. Paris: EU Institute for Security Studies.

Lindstrom, G. (2006). The EU's approach to homeland security: Balancing safety and European ideals. In E. Brimmer (Ed.), *Transforming homeland security:*

U.S. and European approaches. Washington, DC: Center for Transatlantic Relations.

Matlary, J. H. (2009). *European Union security dynamics in the new national interest*. Basingstoke/New York: Palgrave Macmillan.

Miko, F. T., & Froehlich, Ch. (2004). *Germany's role in fighting terrorism: Implications for U.S. policy*. CRS Report for Congress, RL32710. At http://fas.org/irp/crs/RL32710.pdf. Accessed 20 June 2014.

Mitsilegas, V. (2003). The new EU–USA cooperation on extradition, mutual legal assistance and the exchange of police data. *European Foreign Affairs Review, 8*(4), 515–536.

Monar, J. (2010). The rejection of the EU-US SWIFT interim agreement by the European Parliament: A historic vote and its implications. *European Foreign Affairs Review, 15*(2), 143–151.

Monar, J. (2011). The outcomes of the external dimension of the AFSJ. Forms, effectiveness, prospects and specificity. In M. Cremona, J. Monar, & S. Poli (Eds.), *The external dimension of the European Union's area of freedom, security and justice*. Brussels: P.I.E. Peter Lang.

Monet, J.-C. (1993). *Polices et sociétés en Europe*. Paris: La Documentation française.

Murphy, C. C. (2012). *EU counter-terrorism law: Pre-emption and the rule of law*. London: Hart Publishing.

Naftali, T. (2004). Berlin to Baghdad: The pitfalls of hiring enemy intelligence. *Foreign Affairs, 83*(4), 126–132.

NIEUWS Bank (2005, November 7). US Secret Service and Europol partners in fighting organised crime. At http://www.nieuwsbank.nl/en/2005/11/07/R038.htm. Accessed 11 Nov 2005.

Norheim-Martinsen, P. M. (2010). Managing the civil-military interface in the EU: Creating an organisation fit for purpose. In S. Vanhoonacker, H. Dijkstra, & H. Maurer (Eds.), Understanding the role of bureaucracy in the European security and defence policy. *European Integration Online Papers (EIoP)*, 14(1). At http://eiop.or.at/eiop/texte/2010-010a.htm. Accessed 19 Sept 2014.

Papakonstantinou, V., & De Hert, P. (2009). The PNR agreement and transatlantic anti-terrorism cooperation: No firm human rights framework on either side of the Atlantic. *Common Market Law Review, 46*(3), 885–919.

Pauly, R. J., Jr. (2005). French security agenda in the post-9/11 world. In T. Lansford & B. Tashev (Eds.), *Old Europe, new Europe and the US: Renegotiating transatlantic security in the post 9/11 era*. Aldershot/Burlington: Ashgate.

Pawlak, P. (2009). Network politics in transatlantic homeland security cooperation. *Perspectives on European Politics and Society, 10*(4), 560–581.

Pawlak, P. (2010a). Transatlantic homeland security cooperation: The promise of new modes of governance in global affairs. *Journal of Transatlantic Studies, 8*(2), 139–157.

Pawlak, P. (2010b). Made in the USA? The impact of transatlantic networks on the European Union's data protection regime. In M. B. Salter (Ed.), *Mapping transatlantic security relations. The EU, Canada, and the war on terror*. London/New York: Routledge.

Pop, V. (2010, June 25). Breakthrough in EU-US data sharing deal. *EU Observer*. At http://euobserver.com/22/30363?print=1. Accessed 26 June 2010.

Rees, W. (2006). *Transatlantic counter-terrorism cooperation. The new imperative*. Abingdon/New York: Routledge.

Rees, W. (2011). EU-US cooperation on counter-terrorism and the internationalisation of law enforcement. In M. Cremona, J. Monar, & S. Poli (Eds.), *The external dimension of the European Union's area of freedom, security and justice*. Brussels: P.I.E. Peter Lang.

Richelson, J. T., & Ball, D. (1985). *The ties that bind: Intelligence cooperation between the UKUSA countries, the United Kingdom, the United States of America, Canada, Australia, and New Zealand*. New York: Allen and Unwin.

Ripoll Servent, A., & Mackenzie, A. (2012). The European Parliament as a 'norm taker'? EU-US relations after the SWIFT agreement. *European Foreign Affairs Review, 17*(2), 71–86.

Roberts, A. (2003). Entangling alliances: NATO's security of information policy and the entrenchment of state secrecy. *Cornell International Law Journal, 36*(2), 332–338.

Salter, M. B. (2010). The North Atlantic field of aviation security. In M. B. Salter (Ed.), *Mapping transatlantic security relations. The EU, Canada, and the war on terror*. London/New York: Routledge.

Santamato, S., & Beumler, M.-T. (2015). The new NATO policy guidelines on counterterrorism. Analysis, assessment, and actions. In Y. Alexander & R. Prosen (Eds.), *NATO: From regional to global security provider*. Lanham/London: Lexington Books.

Simón, L. (2010). *Command and control? Planning for EU military operations*. Occasional Paper no. 81. Paris: EU Institute for Security Studies.

Smith, S.J. (2013). *The European Union and NATO. Beyond Berlin Plus: the institutionalisation of informal cooperation*. A Doctoral Thesis submitted in partial fulfilment of the requirements for the award of Doctor of Philosophy of Loughborough University, 23 April 2013. At https://dspace.lboro.ac.uk/2134/14341. Accessed 19 Sep 2014.

Spiegel (2014, June 18). Spying together. Germany's Deep Cooperation with the NSA. *Spiegel Online*. At http://www.spiegel.de/international/germany/the-german-bnd-and-american-nsa-cooperate-more-closely-than-thought-a-975445-druck.html. Accessed 20 June 2014.

Stafford, D., & Jeffreys-Jones, R. (2000). *American-British-Canadian intelligence relations 1939–2000*. London/Portland: Frank Cass.

Statewatch (2009, March 24). G6 Meeting (Berlin). Home Department. Written answers and statements. At http://www.statewatch.org/news/2009/sep/g6-meetings-hoc-answer.pdf. Accessed Oct 30, 2009.

Suda, Y. (2013). Transatlantic politics of data transfer: Extraterritoriality, counter-extraterritoriality and counter-terrorism. *Journal of Common Market Studies, 51*(4), 772–788.

Svendsen, A. D. M. (2008a). The globalization of intelligence since 9/11: Frameworks and operational parameters. *Cambridge Review of International Affairs, 21*(1), 129–144.

Svendsen, A. D. M. (2010). *Intelligence cooperation and the war on terror. Anglo-American security relations after 9/11*. Abingdon/New York: Routledge.

SWIFT (2012). *SWIFT Safe Harbor Policy*. At http://www.swift.com/about_swift/legal/compliance/data_protection_policies/swift_safe_harbor_policy.page. Accessed 28 June 2012.

Tardy, T. (2015). *CSDP in action—What contribution to international security?*. Chaillot Paper no. 134. Paris: EU Institute for Security Studies.

Trifunovic, D. (2014). European intelligence cooperation and the Balkan states. *Journal of Mediterranean and Balkan Intelligence, 4*(2), 29–39.

Vermaat, E. (2007, October 8). Homegrown terrorism in Germany: The case of Christian Ganczarski. *Militant Islam Monitor*. At http://www.militantislam-monitor.org/article/id/3204. Accessed 19 Sept 2008.

White House (2001, September 20). The White House Press Statement, Washington, DC. At http://www.yale.edu/lawweb/avalon/sept_11/sept_11.htm. Accessed 8 Jan 2002.

Zaiotti, R. (2012). Practising homeland security across the Atlantic: Practical learning and policy convergence in Europe and North America. *European Security, 21*(3), 328–346.

CHAPTER 9

Network Synergies in the EU Intelligence Community

The long and arduous process of building an intelligence community in the European Union has produced a general institutional framework, well developed strategic intelligence tradecraft and a growing amount of information acquired by EU agencies and bodies. It has been a demanding and contested objective to start from scratch, pulling Member States out of their national silos to construct a networked architecture encompassing numerous dispersed agencies and bodies connected at the EU level by legal provisions and functional arrangements. The hybrid construction of the EU did not facilitate that process. The compartmentalisation of security policies, the 'pillarisation' of legal regulations and political actions, and significant differences between internal security and the external military activities under ESDP/CSDP maintained the second and third pillars instead of softening the divisions and reducing the gap between the two sectors of EU security policy.

The globalisation of risks and threats, and the trans-nationalisation of security governance, have contributed to a gradual change in national perceptions of the security environment and a shift from a state-centric approach to security towards the multi-dimensional construction of security complexes beyond the nation-state (Buzan and Wæver 2003, Chap. 3; Ehrhart et al. 2014b, pp. 120–2). However, these changing national perceptions have often coincided with divergent strategies for coping with security challenges, different assessments of threats and risks, and

A. Gruszczak, *Intelligence Security in the European Union*,
DOI 10.1057/978-1-137-45512-3_9

the growing heterogeneity of the international system (Kirchner 2007, pp. 3–4). In the Europe of the 1990s, the regional response to dynamic global geostrategic transformation was triggered by the reform and reinforcement of integration processes in the political and security dimensions (Buzan and Wæver 2003, pp. 356–64; Kirchner and Sperling 2007, pp. 29–32). Security and defence coordination based on the 'European security identity', together with justice and home affairs cooperation securing the Schengen area and protecting the Union against the serious internal and external threats of terrorism, organised crime or illegal migration, required collective bargaining and arbitration between Member States and relevant EU institutions.

In his study on internal security published in the late1990s by the Western European Union, Alessandro Politi highlighted the need to link the internal and external dimensions of EU security, especially when tackling such problems as terrorism, transnational organised crime or the proliferation of WMD. He argued for the harmonisation of intelligence requirements between the military and law-enforcement agencies of EU Member States (Politi 1997, p. 47). He pointed out potential horizontal connections that could enable increasing collaboration between law-enforcement services, judicial bodies and the military. He stressed that 'it is essential that CFSP and JHA achieve true coordination in instances where the EU has to act at the global level against transnational risks' and claimed that military capabilities could be profitable for law-enforcement agencies in operations and intelligence (Politi 1997, p. 53).

Politi's recommendation has accompanied political debates and institutional developments since the late 1990s. It was not completely fulfilled but found an adequate response in the strategic decisions and actions of the EU intelligence community, which perceived the opportunities and benefits of pooling information sources, developing an institutional framework, improving analytical tradecraft and, finally, generating synergetic effects of networking and intelligence sharing. Numerous obstacles, including national prejudices, security deficits, technological barriers and secrecy rules, have significantly reduced the chance for the EU intelligence community to maximise value added, yet synergetic effects can be found in the 'virtual community' dimension (see Treverton and Gabbard 2008, p. 17), i.e., in communication and interactions between elements of the distorted epistemic community that is EU strategic intelligence.

This chapter provides an insight into how the EU strategic intelligence community has been actively shaped and improved by the establishment, development and consolidation of inter-agency, networked, synergetic connections. Although they emerged in sectoral rather than horizontal settings, they tend to follow a comprehensive approach to knowledge management and intelligence sharing.

Synergy Building: A Nascent Institutionalist Approach

One of the biggest obstacles to a comprehensive model of EU intelligence cooperation has been the institutional architecture, where multiple stakeholders display various competences, manifest varied interests and act at different levels of coordination and integration. Even if, recently, visible progress has been achieved in inter-agency cooperation, particularly in the area of freedom, security and justice, increased cooperation between the former second and third pillars was hardly visible—nor was it, to a considerable extent, even feasible.

The gradual development of an institutional framework for intelligence sharing in the EU has not overcome national impediments to enhanced cooperation in security matters. Prospective intelligence collaboration between EU Member States has effectively been blocked by a mentality of national silos as well as legal and political restrictions. Early attempts to cooperate in the field of information exchange and intelligence sharing were channelled into separate policy areas and followed incompatible time scales (Argomaniz et al. 2015). Military intelligence cooperation since the early 1990s which focused on institutional settings and practical solutions was not accompanied by progress in criminal intelligence sharing at the EU level, which at that time was in its infancy. The pillar structure of the EU erected legal and institutional barriers between the two currents of intelligence cooperation, but Member States seemed quite content with that model (Coosemans 2004, pp. 8–12; Duke 2006, pp. 607–8; Dijkstra 2013, pp. 60–4).

The first proposal for systemic interconnections between the intelligence services of EU Member States was probably formulated by Björn Müller-Wille. He argued for an EU intelligence process built on synthesised military and civil analysis. He ascertained that ‘It is hard to see how the current EU intelligence process could do justice to the early warning function, or estimate and present the consequences of different crisis prevention actions to the Union’s decision-making bodies, without making an analytical synthesis of civil information and military intelligence' (Müller-Wille 2002, p. 80). He observed that the gap between military and civil intelligence is the Achilles' heel of the EU's security policy. Hence, he proposed the establishment within the ESDP structure of a large unit which would work as an organisational node connecting military and civil analysts. Such a node, located 'in-between the Military Staff, the Political and Security Committee and the civil units for analysis organized within the General Secretariat' could produce effective synthesised intelligence for a more efficient and credible warning system and in support of further policy options of the ESDP, including civilian and military missions (Müller-Wille 2002, p. 82).

This proposal seemed premature even in the post-9/11circumstances, when the transatlantic community was mobilised for closer collaboration in the prevention of and fight against terrorism. First of all, there was the call for intelligence networking beyond legal and institutional borders separating the two areas of EU security policies: second-pillar defence and crisis management and third-pillar internal security and border management looked, at that time, fairly naïve. The majority of Member States were not prepared for intensive information exchange and intelligence collaboration. There was a deficit of trust between governments, and fear of misuse, loss or hostile interception of sensitive or classified information paralysed national intelligence services as well as EU efforts at closer cooperation (Bures 2008, pp. 507–9; Fägersten 2010).

The conservative attitude and passive response to EU initiatives proved negative and counterproductive in the wake of the 2004 terrorist bombing in Madrid. Weaknesses and shortcomings in the fragmented intelligence collaboration between national intelligence agencies became evident. There was a strong desire to go beyond the post-9/11 arrangements and launch concrete intelligence cooperation initiatives involving national intelligence and security services as well as EU institutions and bodies. Moreover, it was assumed that the latter would be particularly suited to horizontal arrangements which would prove effective in the fight against terrorism. It was widely believed that threats to the security of the Union and dangers posed by its enemies should be placed on a common denominator.

It was significant that the concept of enhanced horizontal cooperation was associated with the second pillar, and that some analytical capabilities had been developed under the aegis of the High Representative since the early 2000s. In particular, the Joint Situation Centre was frequently mentioned as a would-be intelligence hub in the EU. A partially declassified document drawn up in January 2005 by a ‘trialogue’ of presidencies (Luxembourg, the Netherlands and the UK) provided for SITCEN to have a central position in the General Secretariat of the Council to enable it to provide appropriate customers with intelligence-based assessments and reports. SITCEN could then help to bridge the gap between the CFSP/EDSP and JHA pillars, providing a well crafted internal and external security analysis capability (Council of the EU 2005a, p. 2). It was recommended that intelligence-driven analytical efforts made by counterterrorism groups and other EU bodies operating at the level of intergovernmental cooperation, such as the Terrorism Working Group, horizontal Working Party on Terrorism or the Article 36 Committee in the third pillar, should be more streamlined and focused. Responsibility for accurate, thorough and effective delivery of terrorism-oriented analyses and assessments should rest with SITCEN. However, Europol’s products would keep their own characteristics as intelligence-led criminal analyses on the basis of information provided by national law-enforcement authorities.

The priority for SITCEN was acknowledged by leading EU officials, including High Representative Javier Solana and EU Counter-Terrorism Coordinator Gilles de Kerchove. Solana proposed granting SITCEN competence in ‘the production of intelligence analyses with a view to support EU policy making’ (Solana 2004). De Kerchove, in a short introduction to a report on fusion centres in Europe, argued that: ‘The SITCEN has developed into a unique platform where strategic intelligence produced by the intelligence, security and military services, police information collected by EUROPOL and open sources are integrated and summarised’ (de Kerchove 2010, p. xxi). In a similar vein, Johnny Engell-Hansen, the then Head of the Operations Unit at SITCEN, giving evidence in January 2009 to the UK House of Lords, said: ‘We have established our own open sources intelligence capability within the Situation Centre. Essentially, we are now able to fuse open sources information, diplomatic reporting, military and civilian intelligence into all-sources situation assessments’ (House of Lords 2009, p. 32). William Shapcott, the head of SITCEN at that time, stated emphatically that this unit was an exclusive body with vision and experience of horizontal cross-pillar cooperation in the EU security field. He said: ‘I now go to a host of JHA Committee meetings which I would never have dreamt of a long time ago. De Vries [EU Counterterrorism Coordinator] as well. We are all trying to make sure that the interior ministries see SitCen as something that they own jointly and that works for them' (House of Lords 2005, p. 61). He also asserted that: 'We have been quite careful, even from the beginning, not to formally have it in the Second Pillar. We have played with Solana's double-hatting. […] We are not exclusively a Second Pillar body'(House of Lords 2005, pp. 60–1).

However, SITCEN's real output was less effective and more problematic than initially expected (see Council of the EU 2005b; Shapcott 2008, pp. 26–8, 2011, pp. 121–3). Attempts to practise all-source analysis at SITCEN differed significantly from analogous activities undertaken by national intelligence organisations. Limitations and shortcomings of information exchange and intelligence sharing in the EU lessened the possibilities for the integration of dispersed and diverse information available at the strategic level. Access to classified information was severely restricted which generally limited its usefulness for all-source analysis. The collection and collation of information and intelligence from segmented sources was often onerous and disappointing. Even in strategically important cases an accurate, timely and effective all-source analysis and intelligence assessment was barely feasible (Müller-Wille 2002, pp. 74–8; Fägersten 2008, pp. 63–5).

In an effort to alleviate the deficit of 'sharp' intelligence, all-source analysis has been practised in hubs established around EU agencies and units responsible for cooperation in the established security field. Thus, SITCEN was responsible for threat assessment and situational awareness in EU external missions; the EUMS Intelligence Division for military intelligence; the Crisis Room for crisis management and early warning; Europol and Eurojust for criminal intelligence; and Frontex for situation assessment and risk analysis at the EU external borders.

The expansion of sense-making and intelligence-led bodies in the EU posed a new dilemma associated with the proper distribution of competences and the sound management of information and knowledge at the EU level. It should be underlined that effective management is commonly intertwined with formal political legitimacy. That was why EU Member States decided, on the occasion of the Lisbon reform of EU treaty law, to establish a central coordination unit concatenating law-enforcement services in joint operational efforts and providing them with accurate, timely and useful intelligence support. The Standing Committee on Operational Cooperation on Internal Security (COSI) set up in 2010 (Council of the EU 2010h) became a core element in the institutional framework of EU law-enforcement cooperation, using an intelligence-led approach to promote the EU policy cycle for organised and serious international crime. COSI was also authorised to engage relevant EU agencies and bodies, particularly Europol, in producing threat assessments and providing inputs to the policy-making process specified by the policy cycle. It therefore sought to endow these agencies with resources and capabilities reinforcing EU coordination mechanisms and arrangements focused on early warning, situational awareness and threat assessment.

COSI's role is not only relevant to the coordination of inter-agency activities in the field of internal security and criminal justice. It is equally important to the maintenance of strong, lively and effective working contacts with the Political and Security Committee as a body coordinating and supervising the CSDP. Since 2011, the cooperation between COSI and the PSC has been developed under the heading of 'strengthening ties between CSDP and FSJ (Freedom, Security and Justice) actors', including exchanges of information and mutual support. Administrative arrangements and cooperation schemes between EU law-enforcement and CSDP agencies and units enabled access to and exchange of information and intelligence held by these EU entities.

The COSI–PSC rapprochement came about through a Hungarian initiative seeking a substantial improvement in EU security policy cooperation. Responding to a desire expressed by several Member States, Hungary, which held the presidency of the EU Council in the first term of 2011, made the following specific proposals:

- Enhancing the exchange of personal and strategic information and criminal intelligence between EU civilian crisis-management missions and relevant EU agencies, given that civilian CSDP missions have no legal personality, information is often classified, Frontex is not allowed to exchange personal data and only some of Europol's formal agreements with third countries extend to the sharing of personal data.
- Involving internal security actors, including COSI and the relevant agencies, in the early phase of the planning process during the conduct and review of EU civilian crisis-management missions, including the planning and monitoring of CSDP civilian missions in third countries as well as involvement in the drafting of Crisis Management Concepts and Concepts of Operations.
- Integrating threat and risk assessments supplied by a variety of actors, especially SITCEN's country and thematic reports,

Europol's OCTA and TE-SAT reports, Frontex's risk assessments and the Mission Analytical Capabilities assessments.
- Advocating for the interests of the CSDP and internal security policy actors in the EU's changing data-protection environment through a comprehensive new legal framework on the protection of personal data in the EU.
- Bringing about an immediate and tangible improvement in operational-level cooperation in non-controversial areas, mainly in training (Council of the EU 2011a).

The Hungarian initiative was welcomed by the Council, which recommended work on ways and means of closer cooperation and coordination in the field of EU security should proceed. The Council proposed to convene monthly inter-institutional information meetings of officials from COSI, the General Secretariat of the Council (DGH), EEAS (PSC) and the Commission (DG HOME), to improve planning and information flow. Other services could also be invited, depending on the agenda. Meetings would be hosted either by the presidency or on a rotating basis by the presidency, EEAS and the Commission (Council of the EU 2011b).

In May 2011 EEAS and the Commission followed up the Hungarian initiative with joint proposals to the PSC for strengthening ties between CSDP and internal security actors. These were discussed at the informal PSC-COSI meeting on 1 June 2011 and adopted in December 2011 as the 'Strengthening Ties between CSDP and FSJ' road map. It provided a general framework for common proposals and decisions. Several specific areas for further action were identified, among them comprehensive situational awareness and intelligence support to the EU as well as exchange of information and mutual support. SITCEN was appointed as the leading actor in the field of situational awareness and intelligence. The exchange of information was centred in Europol, and cooperation frameworks with Frontex and Eurojust were to be developed as well as possible collaboration with Interpol (Council of the EU 2011c).

The road map was subject to an annual progress evaluation, and an informal CSDP/FSJ Core Team was set up to monitor its implementation. Progress in this regard was encouraging but not impressive. Although numerous horizontal meetings assembled representatives of EEAS, the General Secretariat of the Council, INTCEN, SATCEN, Europol and Frontex, they focused more on methodological issues, prospects for better information exchange and future undertakings. Formal and practical obstacles to information sharing, especially classified information and personal data, were one of the main problems identified in the course of implementing the road map. It specifically addressed EU agencies in the FSJ area, namely Europol and Frontex, which suffered from the lack of direct exchange of information with EU forces participating in CSDP missions (Council of the EU 2014f, p. 2). Other problems were lack of human resources and reservations as to the reliability of classified document communication systems between the cooperating agencies and bodies (Council of the EU 2014g).

These horizontal initiatives of institutional synergy building, though largely informal and as yet without tangible effects, augur well for future cooperation in information exchange and intelligence sharing, and should be regarded as the starting point of a further search for synergies in EU security policies.

The Single Intelligence Analysis Capacity

The Single Intelligence Analysis Capacity (SIAC) is a functional arrangement of INTCEN and EUMS INT, designed to enhance the quality and increase the number of intelligence products available to EU officials and decision makers.

SIAC was established in January 2007 as a cooperative scheme between the EU Joint Situation Centre and the Intelligence Division of the EU Military Staff (Council of the EU 2008b, p. 98). The idea of bringing together civilian and military intelligence capabilities for more effective and reliable situational assessments and risk analyses came from High Representative Javier Solana in 2006. It addressed the urgent need for a comprehensive approach to the EU's security policies. It was also a reaction to serious shortcomings and intelligence flaws during the 2006 Lebanon war, particularly the deficit of raw intelligence to support SITCEN's production (Engberg 2014, pp. 66–7). Solana's plan was to establish a wider knowledge base for intelligence analysis by pooling civilian intelligence obtained by SITCEN with early warnings and situation assessments provided by the EUMS INTDIV (Jones 2012a, p. 3; van Buuren 2009, p. 10).The objective of these partner entities was to develop a capability for all-source analysis by defining rules of access to information and data acquired both by SITCEN and INTDIV. This was thought to be particularly profitable where there was a pressing necessity to evaluate a crisis or a threat, make situational assessment and risk analysis, or support the decision-making institutions responding to a crisis situation with timely and reliable products (van Buuren 2009, p. 10; Jones 2012a, p. 3).

The SIAC method relied on inputs from civilian and military sources which were collated, compared, analysed and checked against available open information sources. In particular, SIAC was expected to correlate national intelligence deliverables with information and analytical material delivered by EU bodies involved in external actions under the CFSP—civilian and military missions and operations, fact-finding teams and EU delegations as well as Special Representatives and Special Envoys. In its early years, the extended and gradually improving SIAC collaboration scheme brought about wider access to a great variety of information and intelligence. Lt. Gen. David Leakey, Director General in the EU Military Staff in the years 2007–2010, declared with a small dose of exaggeration that 'What is working better and better is the close collaboration between the EUMS Intel Directorate and the Civilian Intelligence machine in the SITCEN. Even Member States push this. It is a developing success story' (IMPETUS 2010, p. 3).

However, the SIAC formula did not entirely meet the needs and demands of Member States. The contribution of national intelligence services did not increase significantly. It also took a long time for reliable communication channels and procedures to be established between SITCEN and INTDIV. Moreover, SIAC did not ensure a fully integrated intelligence analysis process because of the problems with extracting specific data and intelligence from Member States. According to Norheim-Martinsen (2013, p. 98), 'The SIAC does not provide for a fully integrated structure, but ensures that when there is a need for information on a certain issue, for example, an emerging conflict, SITCEN and INTDIR coordinate requests for information, upon which they then base their joint assessment of the situation'. Substantial support comes from EU agencies operating in the internal security field such as Europol and Frontex, which can also exchange analytical material with INTCEN. Also, some parts of the EEAS crisis-management hub are involved in the SIAC workflow. For example, the EU SitRoom has been exchanging its risk assessment lists with SIAC (Manchin 2014, pp. 167–8).

Former Director of Intelligence at EUMS, Brig. Gen. Gintaras Bagdonas (2010, p. 16) assured his readers that 'The SIAC working arrangement is unique for several reasons. Firstly, because it sets the ground for joint intellectual efforts for analysts from the two main EU intelligence entities and prevents duplication; secondly, it has created conditions to implement the new intelligence sharing policy, whereby intelligence contributions provided by MS intelligence organisations are available for both SITCEN and Int[elligence] Dir[ectory] analysts; and finally, these arrangements have been conducted towards achieving the best quality intelligence products corresponding to the EU CSDP requirements.' In similar mood, Ilkka Salmi (2014), the Director of INTCEN, asserted that 'EU INTCEN and EUMS INT together as the Single Intelligence Analysis Capacity (SIAC) form a unique setting for comprehensive joint intelligence assessments, covering both civilian and military, and external and internal, aspects of any given situation'. Józef Kozłowski and José-Miguel Palacios-Coronel (2015, p. 42), former high-ranking officials in EUMS INT and INTCEN, underlined the fact that units they had represented 'have become one of the EU forerunners in the field of producing synergies by a joint civilian-military approach'.

The civilian and military intelligence bodies in the EU strive not only to make the most effective use of the different kinds of information they get from national providers. They also seek to avoid duplicating the acquisition, processing and analysis of information and pre-processed inputs. In the case of national intelligence agencies, both EUMS INT and INTCEN coordinate requests for information with a view to launching and developing a joint intelligence end product (Fägersten 2014, p. 97). Ilkka Salmi argues that SIAC is profitable for INTCEN thanks to its close institutional and personal contact with EUMS INT: 'When we produce our products, most of them are joint production anyway – probably 90 per cent' (Clerix 2014).

SIAC's Military Intelligence System Support (MISS) originally encompassed a joint database administered by EUMS and a network connecting EU INTDIV and SITCEN with national military intelligence services of Member States and other partners (Bagdonas 2010, p. 16). With the establishment of EEAS, an Intelligence Support Architecture (ISA) was formed, its operations set out in the HR/VP's decision no. HR DEC (2012)013 dated 22 June 2012 (classified) (EEAS 2013b, p. 10). This was intended to strengthen inter-agency coordination within EEAS and the European Commission and also improve connections with national intelligence authorities from EU Member States as well as international partners (Kozłowski and Palacios-Coronel 2015, p. 41). Its administrative structure consists of the Intelligence Steering Board (ISB) and the Intelligence Working Group (IWG), assisted by a small secretariat. The ISB is chaired by the HR/VP or the EEAS Executive Secretary-General.

Senior officials from the relevant Managing Directorates of EEAS and, if required, representatives of the General Secretariat of the Council, the Commission and the EU Counter-Terrorism Co-ordinators also sit on the Board. The IWG is a preparatory body for the ISB, co-chaired by the heads of INTCEN and EUMS INT. Again, representatives of the relevant Managing Directorates of EEAS take part in monthly meetings. The secretariat is co-organised and run jointly by EUMS INT and INTCEN (Salmi 2014; Fägersten 2015, p. 7).

The Prioritised Intelligence Requirements (PIR) are the backbone of the ISA. They are adopted every year by the ISB, having been proposed by the IWG following consultations with Member States and, where appropriate, other stakeholders. They are presented as a list of priorities, focus areas and requirements for joint intelligence production at the strategic level. In addition to the PIR, the Steering Board implements organisational and policy measures seeking to improve the overall performance of the ISA and address deficiencies in the EU security field. The IWG, for its part, 'synchronises the tasking of the Single Intelligence Analysis Capacity (SIAC), defines SIAC product range, and develops and monitors a feedback mechanism' (Kozłowski and Palacios-Coronel 2015, p. 42; also Fägersten 2015, p. 7). It is complemented by the SIAC Tasking Mechanism approved by the Intelligence Steering Board (EEAS 2013b, p. 10).

The ISA provides a good example of the opportunities created by the post-Lisbon institutional rearrangement and Member States' belief that closer cooperation between the military and civilian intelligence elements is potential value added to EU security. Notwithstanding national reservations and a deficit of political endorsement, the ISA has framed joint intelligence production in the EU at the strategic level and laid the firm foundations for well structured and increasingly effective cooperation. According to the head of INTCEN, 'this two-level approach to intelligence support ensures a balanced dialogue and constant interaction between the decision-makers and the intelligence providers. It also allows us to arrange the intelligence cycle more appropriately to be able to feed in timely assessments for the policy-making process' (Salmi 2014).

Fusion Centres in the EU

The archipelago of intelligence hubs in the EU has emerged as a considered response to the dispersal of security information around the EU's internal and external dimensions. The main driver behind early efforts to establish intelligence-led analytical units at the EU level was the need to concentrate fragmentary and scattered sources of information. The EU's developing security policies and strategies increasingly require processed information and specialist knowledge for cogent strategic planning and effective decision making. Analytical outputs provided to decision makers by EU bodies had traditionally originated in different institutional and organisational settings employing specific tradecraft and having varied access to information resources and data banks.

The need to 'join up the dots' was a constant headache for EU intelligence units. The fusion method, a holistic approach to intelligence based on all-source information collection and analysis, was regarded as a remedy (Connable 2012, p. 1). Data fusion, according to Buede and Waltz (1998), means 'an adaptive knowledge creation process in which diverse elements of similar or dissimilar observations (data) are aligned, correlated, and combined into organized and indexed sets (information), which are further assessed to model, understand, and explain (knowledge) the makeup and behavior of a domain under observation'. Data fusion usually takes place in a fusion centre. This is a large data clearing house in which information is collected, collated, securely stored, scrutinised, interpreted, analysed and converted into intelligence. Analytical reports (risk analyses, threat assessments, situation trends, critical evaluation) and other intelligence products (such as biographical files, security screening lists, alerts, link and network visualisations, matrices, charts, maps, graphs and other deliverables) are subsequently disseminated to authorised users and stored for further analytical or operational use. The fusion centre offers relatively comfortable working conditions for a variety of agencies and bodies that have traditionally operated as separate entities. The slow yet evident progress in EU security cooperation, especially as regards internal security and border control, but also in the CSDP area, has demanded from EU institutions and Member States more than the responsible, competent and effective management of information and intelligence. Dispersing common assets, hindering intelligence workflow and dismantling institutional efforts at the EU level was no longer acceptable, especially when confronted with challenges and tasks in the areas of counter-terrorism, crisis management and the fight against organised crime. Thus, as described earlier, the military and civilian intelligence sectors within the CSDP approved the format of SIAC. Criminal analysis and information sharing between national law-enforcement services and EU bodies were formally stimulated by EU institutions through the adoption of several legal measures. Council Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offences (Council of the EU 2005c, p. 22) and the Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between national law-enforcement authorities (Council of the EU 2006c, p. 89) required Member States to share all available information and intelligence with both Europol and Eurojust (Rozée et al. 2013, pp. 378–9). These legal measures were intended to strengthen the information workflow between national stakeholders, yet they were also aimed at enhancing the intelligence capabilities of EU agencies, especially Europol's intelligence tasks as provided in the decision establishing this agency. The need to fuse information in an all-source analytical entity was also felt in Frontex. In 2008, the Frontex Situation Centre was created in order to provide a detailed, accurate and up-to-date situational picture of the EU's external borders (Frontex 2015a, b).

These undertakings at least partially proved the potential for synergies between relevant EU agencies and units built on improved intelligence capabilities through standardisation of internal procedures designed to overcome operational obstacles (Svendsen 2011, pp. 531–2). The Lisbon treaty reforms introduced significant changes in the legal and institutional construction of the European Union. Law-enforcement cooperation was strengthened by the EU Internal Security Strategy adopted in early 2010; EU agencies and bodies had new opportunities to manage the growing information flow and achieve significant progress in crime prevention and the tackling of organised crime. A real challenge for law enforcement, however, is posed by obstacles to the integration and collation of scattered sources of information and data. These sources often fall under different jurisdictions, are subject to various procedural and organisational frameworks, and are protected by specific measures.

The application of a fusion centre model to the current EU criminal intelligence hub must take into account existing intelligence sharing and law-enforcement collaboration systems which tend to use all-source analysis to produce strategic intelligence, threat assessments and situational reports. Europol is predestined to perform the role of a fusion centre given its tasks, competences and resources. As Patrick G. Byrne, Europol Senior Representative in Washington, D.C., aptly stated, 'Europol itself could be described as a European fusion center—ready, willing, and able to support its international partners and colleagues. It is a major international fusion center collecting, collating, and analyzing data and delivering support to EU member states and its operational and strategic partners' (Byrne 2013, p. 65).

In this view, Europol is an EU agency in charge of criminal intelligence analysis and intelligence support in transnational law-enforcement operations. However, its databases are fed mostly by national police services, supplemented by open-source information from the media, publicly available materials and commercial analytical products. Data and intelligence acquired and stored by EU agencies and units can compensate for the lack of secret government intelligence, but sensitive criminal intelligence held by such agencies as Frontex, INTCEN or SATCEN, is subject to specific regulations regarding security clearance, data encoding, data transmission, user authentication and so on.

In spite of these drawbacks, Europol appears to possess the organisational resources, experience, practical knowledge and international reach necessary for a fusion centre (Busuioc and Groenleer 2013, p. 293). Its complex, state-of-the-art computerised database and communication system receives information and data from national law-enforcement and/or internal security agencies of Member States and, when necessary, third countries and organisations (Mounier 2009b). Their inputs are verified, selected and stored in Europol's files and databases. EU agencies and bodies like INTCEN, Frontex, Eurojust and the office of the EU Counter-Terrorism Coordinator also contribute relevant data. Europol collates these data with information mined from public media and other open sources: government documents; reports from public organisations and the private sector; academic publications; so-called grey literature (unpublished written material or studies published outside publicly available sources, often lacking peer review); journals and magazines; and news agency reports and newspapers. In cases of contradictions or ambiguities, intelligence extracted from open sources is cross-checked against Member States' inputs. The results are integrated with the policy cycle for organised and serious international crime.

Synergetic Network Arrangements: Towards a Comprehensive Approach

The original fusion centre model assumed a solid institutional and organisational groundwork, a secure working environment, a concentrated information flow, the maximisation of synergies and intensified efforts by analysts and intelligence producers. Within the EU criminal intelligence hub, Europol represents this model. However, there is scope for synergetic intelligence networks extending beyond formal institutional settings and enabling the fusion and analysis of dispersed, multi-source information and intelligence. Inter-institutional connectivity must be tackled in the context of complex communication networks, the soft competences of EU institutional actors and the often rigid stances exhibited by Member States.

The EU intelligence community could be depicted as a virtual networked arrangement enabling the fusion of data and information acquired from scattered sources to produce complete and timely intelligence estimates and assessments of the main threats and risks to EU security. An EU virtual intelligence hub (EU VIH) closely connects the EU agencies and units that are practically involved in strategic intelligence analysis—Europol, Frontex and the EU Intelligence Analysis Centre—which employ their own specific tradecraft and are linked to other sectoral EU intelligence arrangements active in the CFSP/CSDP and AFSJ policy areas. Rather than a single physical location, an institutional network established at EU level guarantees a relatively secure, stable and professional working environment for intelligence tradecraft. Rather than a head unit with strong political position and wide operational capabilities, this model relies on working arrangements, substantial levels of mutual confidence and efficient communication networks. EU VIH resembles a macro-hub linking existing sectoral fusion establishments scattered throughout the wide area of EU security. Political, legal and logistical impediments over matters of internal security, crisis management and defence preclude the centralisation of strategic intelligence and the institutional fusion of information related to security threats and risks.

EU VIH is, then, a working arrangement maximising information and intelligence inputs acquired and processed by national authorities from EU Member States and third parties or extracted from overt sources. This ‘pooling and sharing’ arrangement is the rationale for intense intelligence-led cooperation aiming to identify main threats, detect sources of risks and support all-source intelligence analysis.

The first hurdle in integrating these agencies and units is their organisational autonomy, reflected in the scope of their competences and degree of independence within the EU institutional framework. It determines the availability of information as well as the quantity of data transferred to authorised customers in EU agencies and units.

The essence of EU VIH is that its interconnected hubs enable a constant formalised information workflow and intelligence sharing, but it lacks a central data clearing house. Scattered intelligence originators make only partial use of synergetic connections between the institutional nodes. The division lines between intelligence hubs remain clear-cut and almost impassable; all-source analysis within the EU intelligence community is still the frame of reference, Although former High Representative Catherine Ashton acknowledged that 'the EU INTCEN serves as the EEAS' intelligence hub', the Council later resolutely declared that 'neither the SITCEN, nor any other component of the EEAS, is an "intelligence service". The High Representative has no intention to establish an "intelligence service" as part of the EEAS' (European Parliament 2010a). Later official statements rejecting the creation of an EU intelligence agency reaffirmed the lack of political consensus among Member States.

Comprehensiveness is considered by EU officials as the key element of EU crisis prevention and crisis management, highly relevant in cases of complex crises and breakdowns with serious and long-term political, military, economic, diplomatic and humanitarian consequences (Vimont 2014, p. 36). In May 2014, the Council pointed out that the comprehensive approach to EU security policy should stem from early, coordinated and shared analysis of the security environment. Joint analyses should contribute to decision making, providing shared context analysis, particularly when civilian and military expertise is needed and civilian–military synergies can be generated (see Faria 2014, pp. 11–12). The Council referred to inter-agency coordination and connectivity as the essential element in the EU's comprehensive approach to knowledge management and information sharing, focusing on the ongoing process of approximation between the CSDP and FSJ agencies: 'The Council also underscores the need to continue to strengthen the ties between CSDP and the areas of Freedom, Security and Justice (FSJ) and more effectively develop synergies between CSDP actions with FSJ actions as well as actions carried out in other EU domains' (Council of the EU 2014h, p. 3).

The comprehensive approach to intelligence cooperation in the EU assumes that traditional boundaries between security fields and intelligence disciplines will increasingly have less relevance, enabling EU institutions and agencies and Member States to make the best use of available resources and work out a responsive and adaptive approach to emerging challenges (Haag and Anaya 2011, p. 9). There is a strong political consensus among Member States on the need to develop and consolidate arrangements that can improve awareness of challenges and effective responses without prejudice to national security interests and sovereign rights.

Inter-agency information exchange takes place at different levels and the contribution of individual agencies to intelligence output also varies. The potential for synergetic connections is still insufficiently exploited. In addition to the reservations of Member States, the lack of mutual confidence and technological barriers, the sharing of EU classified information and intelligence products built on classified national inputs is contested. In practice, OSINT deliverables barely fill the gaps left by national intelligence services, underscoring the importance of a comprehensive approach to intelligence cooperation in the EU. The existing components of the EU strategic intelligence community provide a solid basis for developing more advanced forms of cooperation. SIAC, inter-agency connections, fusion mechanisms and all-source analytical solutions should be regarded as structural and functional components of the intelligence community network architecture. The ability to generate added value from the information resources and analytical skills is clear in the area of EU security but it remains a long way from a genuine, fully fledged and comprehensive model of security governance in the EU.

Bibliography

Argomaniz, J., Bures, O., & Kaunert, C. (2015). A decade of EU counter-terrorism and intelligence: A critical assessment. *Intelligence and National Security, 30*(2-3), 191–206.

Bagdonas, G. (2010). Evolution of EUMS intelligence directorate and a way ahead. *Impetus. Bulletin of the EU Military Staff, 9*, 16.

Buede, D., & Waltz, E. (1998). Data fusion. In *McGraw Hill Encyclopedia of science and technology*. New York: McGraw Hill.

Bures, O. (2008). Europol's fledgling counterterrorism role. *Terrorism and Political Violence, 20*(4), 498–517.

Busuioc, M., & Groenleer, M. (2013). Beyond design: The evolution of Europol and Eurojust. *Perspectives on European Politics and Society, 14*(3), 285–304.

Buzan, B., & Wæver, O. (2003). *Regions and powers. The structure of international security*. Cambridge: Cambridge University Press.

Byrne, P. G. (2013). Increased globalization of organized crime and terrorism: Europol and the EU perspective. *The Police Chief Magazine, LXXX*(8). At http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=print_display&article_id=3018&issue_id=82013. Accessed 18 Mar 2015.

Clerix, K. (2014). Ilkka Salmi, the EU's spymaster. *Mondiaal Nieuws*, 4 March. At http://www.mo.be/en/interview/ilkka-salmi-eu-s-007. Accessed 10 June 2014.

Connable, B. (2012). *Military intelligence fusion for complex operations. A new paradigm*. Santa Monica: RAND Corporation.

Coosemans, Th. (2004). *L'Union Européenne et le renseignment: Perspectives de coopération entre les états membres.* Rapport du GRIP 3. Bruxelles: Groupe de recherche et d'information sur la paix et la sécurité.

Council of the EU (2005a, January 11). Note from presidency and the delegations from the Netherlands and United Kingdom to Article 36. Subject: EU SitCen work programme, doc. 5244/05 EXT 1, Brussels.

Council of the EU (2005b, December 20). EU SitCen work programme, doc. 5244/05, Brussels.

Council of the EU (2005c, September 29). Council decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences. *Official Journal of the European Union, L 253.*

Council of the EU (2006c, December 29). Council framework decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. *Official Journal of the European Union, L 386.*

Council of the EU (2008b, April 25). Annual report from the Council to the European Parliament on the main aspects and basic choices of the CFSP, doc. 8617/08, Brussels.

Council of the EU (2011a, January 25). Note from Presidency to Standing Committee on operational cooperation on internal security (COSI). Tightening links between the external and internal aspects of EU security, doc. 5620/11, Brussels.

Council of the EU (2011b, May 30). Draft working method for closer cooperation and coordination in the field of EU security, doc. 9125/3/11 REV 3, Brussels.

Council of the EU (2011c, May 10). Strengthening ties between CSDP and FSJ actor, doc. 9930/1, Brussels.

Council of the EU (2014f, December 10). Political and Security Committee (PSC) Standing Committee on operational cooperation on internal security (COSI)—Summary of discussions held on 11 November 2014, doc. 16372/14, Brussels.

Council of the EU (2014g, October 29). Strengthening ties between CSDP and FSJ: Road map implementation third annual progress report, doc. 14854/14, Brussels.

Council of the EU (2014h, May 12). Council conclusions on the EU's comprehensive approach. Foreign Affairs Council meeting, Brussels. At http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/142552.pdf. Accessed 16 May 2014.

De Kerchove, G. (2010). Future challenges in the fight against terrorism. In Belgian Standing Intelligence Agencies Review Committee (Ed.), *Fusion centres throughout Europe. All-source threat assessments in the fight against terrorism*. Antwerp/Oxford/Portland: Intersentia.

Dijkstra, H. (2013). *Policy-making in EU security and defense. An institutional perspective*. Basingstoke/New York: Palgrave Macmillan.

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

EEAS (2013b). Answers by the High Representative/Vice President Catherine Ashton to the written questions of the Committee on budgetary Control. At http://www.europarl.europa.eu/document/activities/cont/201301/20130107ATT58545/20130107ATT58545EN.pdf. Accessed 7 May 2014.

Ehrhart, H.-G., Hegemann, H., & Kahl, M. (2014b). Putting security governance to the test: Conceptual, empirical, and normative challenges. *European Security, 23*(2), 119–125.

Engberg, K. (2014). *The EU and military operations: A comparative analysis*. London/New York: Routledge.

European Parliament (2010a, 4 March). Written question E-1131/2010 by Martin Ehrenhauser (NI) to the Council. Subject: EU Observer article of 22 February 2010. At http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-1131&language=EN. Accessed 8 Mar 2013.

Fägersten, B. (2008). *European intelligence cooperation: Drivers, interests and institutions*. SIIA Papers, br. 6. Stockholm: The Swedish Institute of International Affairs.

Fägersten, B. (2010). Bureaucratic resistance to international intelligence cooperation—The case of Europol. *Intelligence and National Security, 25*(4), 500–520.

Fägersten, B. (2014). European intelligence cooperation. In I. Duyvesteyn, B. de Jong, & J. van Reijn (Eds.), *The future of intelligence—Challenges in the 21st century*. Abingdon/New York: Routledge.

Fägersten, B. (2015). *Intelligence and decision-making within the Common Foreign and Security Policy*. European Policy Analysis no. 22. Stockholm: SIEPS.

Faria, F. (2014). *What EU comprehensive approach? Challenges for the EU action plan and beyond*. ECDPM Briefing Note no. 71. Maastricht: ECDPM. At http://ecdpm.org/wp-content/uploads/BN71-What-EU-Comprehensive-Approach-October-2014.pdf. Accessed 17 Dec 2014.

Frontex (2015a). Frontex Consultative Forum on fundamental rights background note for the public call for applications. At http://frontex.europa.eu/assets/Attachments_News/CF_call_documents/Background_doc_for_public_call_FINAL.pdf. Accessed 1 July 2015.

Frontex (2015b). Frontex Consultative Forum on Fundamental Rights. Second Annual Report 2014. At http://frontex.europa.eu/assets/Partners/Consultative_Forum_files/Frontex_Consultative_Forum_annual_report_2014.pdf. Accessed 5 Sep 2015.

Haag, D., & Anaya, C. B. (2011). The first ten years of military Intelligence Support for the work of the EU. *Impetus. Bulletin of the EU Military Staff, 11*, 8–9.

House of Lords (2009). *Civil protection and crisis management in the European Union. Report with Evidence*. HL Paper 43. London: The Stationery Office.

House of Lords (2005). *After Madrid: the EU's response to Terrorism. Report with Evidence*. HL Paper 53. London: The Stationery Office.

IMPETUS (2010). Interview with DGEUMS—LT Gen Leakey. *Impetus. Bulletin of the EU Military Staff, 9*, 2–4.

Jones, C. (2012a). Secrecy reigns at the EU's Intelligence Analysis Centre. *Statewatch, 22*(4), 3–6.

Jones, F. L. (2012b). Strategic thinking and culture: A framework for analysis. In J. B. Bartholomees Jr. (Ed.), *U.S. Army War College guide to national security issues. Volume II: National security policy and strategy* (5th ed.). Carlisle: U.S. Army War College.

Kirchner, E. J. (2007). Regional and global security. Changing threats and institutional responses. In E. J. Kirchner & J. Sperling (Eds.), *Global security governance: Competing perceptions of security in the 21st century*. London/New York: Routledge.

Kirchner, E. J., & Sperling, J. (2007). *EU security governance*. Manchester: Manchester University Press.

Kozłowski, J., & Palacios-Coronel, J.-M. (2015). The single intelligence analysis capacity within the European Union. In J. Rehrl & G. Glume (Eds.), *Handbook on CSDP missions and operations*. Vienna: Directorate for Security Policy of the Federal Ministry of Defence and Sports of the Republic of Austria.

Manchin, J. (2014). Overview of crisis rooms. In P. Pawlak & A. Ricci (Eds.), *Crisis rooms: Towards a global network?* Paris: EU Institute for Security Studies.

Mounier, G. (2009b). Europol: A New Player in the EU External Policy Field? *Perspectives on European Politics and Society*, 10(4), 582–602.

Müller-Wille, B. (2002). EU intelligence co-operation. A critical analysis. *Contemporary Security Policy, 23*(2), 61–86.

Norheim-Martinsen, P. M. (2013). *The European Union and military force. Governance and strategy*. Cambridge: Cambridge University Press.

Politi, A. (1997). *European security: The new transnational risks*. Chaillot Paper no. 29. Paris: Institute for Security Studies of the WEU.

Rozée, S., Kaunert, C., & Léonard, S. (2013). Is Europol a comprehensive policing actor? *Perspectives on European Politics and Society, 14*(3), 372–387.

Salmi, I. (2014). Multilateral intelligence cooperation in the EU. *GNOSIS. Rivista Italiana di Intelligence, 2*. At http://gnosis.aisi.gov.it/Gnosis/Rivista39.nsf/ServNavig/24. Accessed 11 June 2015.

Shapcott, W. (2008). The role of the EU Joint Situation Centre in the European Security Architecture. In *Terrorismusbekämpfung in EuropaHerausforderung für die Nachrichtendienste. Vorträge auf dem 7. Symposium des Bundesamtes für Verfassungsschutz am 8. Dezember 2008*. Köln: Bundesamt für Verfassungsschutz.

Shapcott, W. (2011). Do they listen? Communicating warnings: An intelligence practitioner's perspective. In Ch. de Franco & Ch. O. Meyer (Eds.), *Forecasting, warning, and responding to transnational risks*. Basingstoke/New York: Palgrave Macmillan.

Solana, J. (2004, June 8). Summary of remarks by Javier Solana, EU High Representative for CFPS on Terrorism and Intelligence Co-operation, Brussels. At http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/declarations/80852.pdf. Accessed 20 Mar 2013.

Svendsen, A. D. M. (2011). On 'a continuum with expansion'? Intelligence co-operation in Europe in the early twenty-first century. *Journal of Contemporary European Research, 7*(4), 520–538.

Treverton, G. F., & Gabbard, C. B. (2008). *Assessing the tradecraft of intelligence analysis*. RAND Technical Report TR-293. Santa Monica: RAND Corporation.

van Buuren, J. (2009). *Secret Truth. The EU Joint Situation Centre*. Amsterdam: Eurowatch.

Vimont, P. (2014). The European External Action Service and complex crises. In P. Pawlak & A. Ricci (Eds.), *Crisis rooms: Towards a global network?* Paris: EU Institute for Security Studies.

CHAPTER 10

EU Intelligence Oversight

The issue of democratic oversight of intelligence services raises many controversies and poses some challenging questions about appropriate normative frameworks, procedures and instruments. It goes without saying that intelligence services and their international forms of cooperation are to a considerable extent shrouded in secrecy, creating significant obstacles to any form of monitoring, control, supervision or oversight (Gill and Phythian 2012, pp. 170–2). The intelligence sector often has to defend itself against close monitoring and careful observation by the media and NGOs sensitive to issues of privacy, transparency and accountability. It seeks exemption from thorough review for the sake of its robustness, effectiveness and reliability. It is motivated by its unique capacities and exclusive entitlement to carry out secret activities concerning vital security issues and protecting public order and national interests. However, the 'exclusiveness' of the intelligence sector may generate serious risks and, sometimes, direct threats to the legitimate authorities, the legal order in the state and, last but not least, international relations. Intelligence can pose serious moral and ethical dilemmas in view of its contested tradecraft, secrecy and exclusiveness, and activities that may be detrimental to privacy and individual freedoms (Herman 2004; Erskine 2004; Sepper 2020; Gill and Phythian 2012). The danger of the emergence of the 'state within a state' has urged civil society and citizens' representative institutions to determine criteria, norms and procedures of democratic oversight making the intelligence sector accountable to state authorities and to civil society.

A. Gruszczak, *Intelligence Security in the European Union*,
DOI 10.1057/978-1-137-45512-3_10

Oversight, Control and Accountability

Oversight is defined as the thorough, careful and structured scrutiny of an entity (individual, organisation or network) that aims to evaluate its compliance with binding rules, principles or criteria, such as effectiveness, validity or transparency (Baker 2008, pp. 201–2). It includes formal and informal, general and detailed measures and procedures covering all aspects of the entity's behaviour or performance or focusing on specific areas (Wills et al. 2011, p. 41). It also entails informal and formal scrutiny by the legislature of the observance of constitutional principles, legal norms and regulations. Oversight is closely tied to the notion of accountability. Following Bovens, accountability may be defined as a relationship between an actor and the organisational environment in which the actor is obliged to explain his or her conduct, justify past, present and future decisions and actions, respond to questions and charges and accept the full consequences of his or her behaviour (Bovens 2007a, b; Bovens et al. 2010, p. 35). Accountability from an institutional perspective is the checking and overseeing of the established patterns of agents' behaviour. In the functionalist perspective, it is a precondition of the legitimacy, transparency and efficiency of actors in a pre-defined setting promoting mutually beneficial cooperation (Grant and Keohane 2005, pp. 31–2; Keohane 2006, p. 76; Bovens 2010, pp. 954–5). In the normative perspective, it is associated with mechanisms and procedures for enforcing rules and executing sanctions in the event of a breach of the normative order. Control and punishment underpin the regulatory function of accountability as a relationship, ensuring the rule of law and preventing abuse of power in a complex governance system (Benz et al. 2007, p. 443; Trechsel 2010, pp. 1052–3). Accountability mechanisms are territorially bounded because of the relatively narrow scope of international cooperation between national oversight and review bodies (Leigh 2011, p. 4).

Oversight, control and accountability quite often address the problem of 'abuse of power', or in more practical terms, the stretching of competences beyond their formal limits, legal boundaries or organisational frameworks. Leigh put forward three persuasive arguments for the legal oversight and supervision of international intelligence cooperation (Leigh 2011, p. 7). First, intelligence activities take place within a legal framework which makes them subject to general and specific provisions. Likewise, intelligence agencies are not only politically dependent but are also bound by legal norms which are overseen by relevant constitutional bodies. Second, the national intelligence institutions and international arrangements they establish and maintain must observe international law, especially its humanitarian aspects, and strictly follow the principles of lawfulness and certainty. Third, intelligence officials must assume legal liability and responsibility for their decisions and activities.

The often contentious issue of oversight and control has also been identified with regard to intelligence cooperation in the EU. Although the powers conferred on EU institutions and agencies making up the intelligence community are considerably limited (see Bono 2006, p. 442), the density of sense-making and intelligence networks, and the comprehensive approach to the management and political supervision of information exchange and intelligence sharing makes it desirable, indeed necessary, to determine multiple mechanisms of oversight and control in intelligence cooperation at the EU level. Nevertheless, individual Member States have national patterns of oversight and scrutiny in place that can act as a springboard for enhanced control and supervision of EU agencies and bodies involved in intelligence cooperation.

In most EU Member States international intelligence cooperation is a politically sensitive issue and 'an under-scrutinised area of services' work' (Leigh 2015, p. 1). As Gill and Phythian argue (2012, p. 177), security intelligence is 'low visibility work' with extensive scope for discretion. There are many reasons: the sovereignty principle, the predominance of national oversight authorities, the soft competences of international scrutiny bodies, restricted access to information and lack of trust. National institutions are responsible for control and oversight in accordance with binding legal regulations. Information, data or intelligence entrusted to supranational agencies and loaded into computer information systems connecting numerous national users in a central hub managed by EU institutions have already been checked for their availability to external actors. Oversight therefore entails: management of data stored in EU information systems; supervision of authorities responsible for the proper handling of information received and the delivery of intelligence products; control of the application of EU norms regulating access to information, in particular that covered by a confidentiality clause; and checking whether information and intelligence products are strictly related to categories permitted by the law.

The European intelligence community does not possess autonomous operational capabilities and as such avoids controversial and risky activities which could result in public protests or political skirmishes. Hence, no dramatic decisions and disputed operations, such as covert actions, eavesdropping or infiltration, have occurred. However, there have been many controversies surrounding the management of information by EU agencies and bodies, the transfer of sensitive data to third countries and the control of the way information and intelligence is used by EU agencies and units; these have stimulated political discussion and proposals for enhancing oversight and scrutiny of the EU intelligence community. Generally, oversight and accountability address the following issues:

- protection of information, especially personal data;
- vertical accountability of EU agencies and bodies;
- horizontal oversight on EU legal grounds.

In a democratic community, which the European Union certainly is, democratic oversight executed by institutions endowed with constitutional prerogatives is considered a prerequisite for the legitimacy and accountability of executive power. Oversight and control over intelligence services is seen as a safeguard against potential harm to democratic governance, civil liberties and fundamental rights through the abuse of powers and competences granted to the intelligence authorities. Given that the management of intelligence services depends on the executive, intelligence leadership and its subordination to the government risks becoming politicised. The worst-case scenario would involve the head of an executive branch or government using intelligence apparatus as a tool to weaken the opposition and safeguard its own particular, and not the national, interests. The risk of a government getting out of control and creating a 'state within the state' is often seen by the public as one of the biggest threats to democratic governance (Leigh 2007, p. 68). Nevertheless, even the most radical opponents of the 'pervasive' secret services acknowledge the need to have state institutions protecting critical information sources and shielding the central authorities from dangerous interference. As Caparini (2007, p. 4) aptly put it: 'The quest of intelligence control and oversight in the democratic state, then, is to enable agencies to produce effective security intelligence while ensuring that they operate within the law and in a way that is consistent with democratic norms and standards'.

An analysis of the oversight and accountability of the EU intelligence community is highly demanding in terms of methodology. The generic model of intelligence oversight and democratic accountability applied to individual states and their political regimes does not necessarily fit the structure and logic of EU intelligence cooperation, which has evolved from dispersed and varied forms of cooperation to a genuine organisational form of intelligence sharing. Some of the interesting conceptual proposals in this area do not meet the EU's current determinants, tasks and challenges. Müller-Wille's conception of the hierarchical accountability of EU intelligence cooperation is a telling example. It focuses on the question of who the political 'master' is at the EU level (Müller-Wille 2006, pp. 109–10), highlighting the institutional framework of cooperation and assuming a relatively low level of intelligence sharing with the participation of EU agencies and units.

For the purpose of the present study, the explanatory power and descriptive value of the tri-dimensional accountability concept seem more suitable. It emphasises the peculiar aspects of the 'distorted community' of intelligence stakeholders in the EU, which derives from its heterogeneous structure, networked system of interconnected hubs, and intersecting identities, competences and loyalties. It also frames the complexity of EU intelligence control mechanisms in the context of tensions between national scrutiny and supranational oversight.

Tri-dimensional Accountability

Accountability and oversight in democratic regimes have been extensively discussed by outstanding representatives of 'transitology' and 'consolidology', in other words, scholars developing theoretical approaches to social and political change. Guillermo O'Donnell introduced the concept of two dimensions of accountability: vertical and horizontal (O'Donnell 1994, p. 64). The former concerns the sources of legitimate authority and the relationship between actors participating in power distribution (i.e., from citizens to elected leaders); the latter refers to autonomous agencies capable of calling into question and eventually punishing the misuse of prerogatives or the abuse of power by a public actor (Waldrauch 1998, pp. 1–2). Robert Pastor (1999, p. 124) added the third dimension of accountability: international observation and supervision 'enhancing vertical accountability by making sure elections are successful and strengthening the horizontal axis by calling encroaching institutions to account for their actions'.

Marina Caparini adopted the concept of tri-dimensional accountability in her analysis of intelligence services. Starting with the vertical dimension, she emphasised the importance of the executive as the branch of the state responsible for tasking and directing intelligence services. Representatives of the executive (the president, the head of government or a minister responsible for the intelligence sector) can set policy guidelines, determine administrative systems or directly instruct the head and senior management of intelligence agencies. They can demand access to relevant information held by the services for the sake of national security and vital national interests. Top-down hierarchical control and supervision are also enforced by the head of the intelligence sector or directors of individual agencies. An internal affairs department ensures the proper discharge of duties by intelligence officers and intervenes in any case of misconduct. Exceptionally in intelligence services, bottom-up accountability in the form of 'whistleblowing' is an internal mechanism to draw public attention, or even the state authorities' concern, to mismanagement, malfunctioning or direct threats to national security or the public interest. Self-accountability and exact compliance with professional norms and administrative directives occur more frequently (Caparini 2007, pp. 10–11). The vertical dimension also involves non-state actors: citizens, non-governmental organisations, advocacy groups and media. None of them is formally entitled to supervise intelligence authorities. They conduct 'undersight' (*sousveillance*), monitoring official surveillance practices, expressing concerns when appropriate (van Buuren 2013, p. 250) and alerting the public when fundamental interests or civil liberties are in jeopardy. The media as the 'fifth power' play a prominent role due to their much wider access to information and their capacity to contact the representatives of state authorities, including the intelligence sector. They can also articulate public opinion, voice citizens' concerns and provide feedback to state security institutions and authorities (Caparini 2007, pp. 12–13).

The horizontal dimension consists of inter-institutional connections and is determined by the distribution of competences and duties among parallel power branches. Separation of powers and a system of checks and balances are the foundations of democratic government, safeguarding constitutional principles and national security. Intelligence services, with their specific role in national security policy and strategy, interact differently with each of the branches of state power. The steering and management functions performed by the executive are subject to internal control mechanisms that sometimes involve politicisation and partisanship. Consequently, the legislature acts as the 'guardian' of democratic control and oversight. Parliamentary scrutiny is often regarded as the most effective means of supervision of intelligence institutions and as a corrective mechanism in respect of the intelligence apparatus. Parliament establishes the legal framework for the intelligence sector, sets the competences, rights and duties of intelligence services, exercises general oversight and decides on financial resources. Parliamentary committees can request information from representatives of intelligence services and organise hearings (Caparini 2007, p. 13). Parliamentary oversight does, however, have some shortcomings. Intelligence officials may decline to provide information requested in the interests of national security. Secrecy is frequently used as a weapon against inquisitive MPs. Political rivalries may also prevail over the real need to scrutinise intelligence institutions (Baker 2008, p. 200), which may lead to an instrumental and biased approach to the intelligence sector.

The role of the judiciary is peculiar due to its prerogative to monitor actions of the other branches and particularly to prevent the executive from exercising power arbitrarily (Leigh 2007, pp. 75–6). Judicial review gives the courts the power to interpret laws and veto actions which undermine constitutional and legal order (Caparini 2007, p. 15). Independent oversight is an important addition to the vertical configuration of accountability. The offices of ombudsman, data-protection supervisor or national auditor can investigate procedural irregularities and administrative failings.

The third dimension of accountability addresses the impact of international actors on the functioning of national intelligence agencies. Caparini argues that the role of the international community is increasingly significant in spite of the sovereignty principle and the protective measures adopted by national governments. Intergovernmental organisations, such as the Council of Europe or NATO, international courts, like the European Court of Human Rights, and even international NGOs can exert a direct influence on national intelligence services. They can reveal secret information and launch international investigations (as in the case of the so-called CIA rendition flights in collaboration with several European countries). They can even set some standards with regard to oversight and accountability (Caparini 2007, pp. 16–17).

The tri-dimensional accountability model fits the EU intelligence community well given the data, information and analytical material that underpin it. Respect for ‘national ownership’ of information and intelligence transmitted to the relevant EU agencies and units has a tremendous practical impact on oversight and control. For the governments of Member States, their presence in the Council of the EU and its working bodies is not always sufficient. They seek to tighten their grip on information management in the security field through the establishment of joint supervisory authorities. Equally, national supervision may be strengthened by national parliamentary oversight insofar as the required EU legislation is adopted.

In the vertical setting, the activities of social actors, advocacy groups and media are important, as they indicate the areas exempted from 'normal' monitoring and control and thereby posing certain risks to fundamental rights, civil liberties and democratic politics. *Sousveillance* 'focuses on enhancing the ability of people to access and collect data about their surveillance and to neutralize surveillance' (Mann et al. 2003, p. 333). Several NGOs, independent advocacy groups and media outlets, such as Statewatch, the Transnational Institute, EU Observer.com or Euractiv.com have been systematically observing developments in EU intelligence cooperation.

Vertical Intelligence Oversight in the EU

The European intelligence community was established by Member States which took advantage of existing legal and organisational capabilities and engaged various EU institutions and agencies in information exchange and analysis for the purposes of security, crisis management and public order. Despite the ever-increasing capabilities of EU bodies, advanced intelligence tradecraft and synergetic connections within the EU, intelligence cooperation is heavily dependent on national strategies, policies and inputs. This is less obvious in the strategic dimension, where horizontal networks of knowledge sharing and strategic forecast connect various sources of intelligence and enable the flow of diversified information resources. The vertical setting, especially with regard to oversight mechanisms, highlights the national interests of Member States as well as political and legal constraints. The principle of 'sovereign ownership' of information and intelligence products handed over by national authorities for further use by EU institutions and agencies is the cornerstone of EU cooperation. Therefore, information sharing and the delivery of intelligence products remains under the direct supervision of relevant national authorities. This is especially relevant to military intelligence, which is subject to stringent safeguards enforced by national authorities. The configuration of the EU security field, where representatives of national governments are involved in the supervision and control of agencies belonging to the EU intelligence community, reflects the intergovernmental nature of intelligence cooperation, particularly with regard to the criminal intelligence hub and the three agencies operating there: Europol, Eurojust and Frontex.

The military hub is effectively outside the supervision and control of EU institutions and bodies. The Intelligence Directorate of the EU Military Staff is subordinated to the EU Military Committee, composed of representatives of Member States' chiefs of defence. The EU Military Committee responds to the Political and Security Committee, guaranteeing that representatives of governments exert a direct influence on military co-ordination and keep control of strategic developments in military security and crisis management. No joint supervisory body has been created; any form of supervision or monitoring is up to national representatives of the government or the military staff. The case of INTCEN is distinct: it provides intelligence support for CSDP missions and operations on the basis of information and analyses delivered by national civilian intelligence services. Its dubious legal basis has blurred the limits of accountability and in practice it avoids democratic scrutiny. Instead, a well elaborated mechanism of horizontal accountability, executed by the High Representative, has been implemented and improved (Clerix 2014). The diplomatic and crisis-management hubs operate within the institutional framework of EEAS. The HR/VP keeps the mechanisms, channels and procedures of intelligence sharing under constant supervision without detriment to the security and foreign affairs interests of the Member States.

Vertical oversight is much more developed in the area of freedom, security and justice, where agencies are subject to review and government bodies are inspected as provided by the Council of the EU or appointed by the Management Board. The Lisbon treaty established the Standing Committee on operational cooperation on internal security (COSI), which sits at the same level as the Political and Security Committee in the CSFP/CSDP fields and also holds a strategic position with regard to information management and intelligence sharing. In particular, COSI is responsible for promoting the principles of intelligence-led policing and improving information sharing in the internal security field. COSI monitors developments in the field at the strategic and policy-shaping levels, sets priorities for the agencies and contributes to strategic guidelines adopted by the Council (Council of the EU 2015).

The EU criminal intelligence hub is also monitored by representatives of independent national supervisory bodies which make up a joint supervisory authority. This body controls the accountability of agencies and supervises the large-scale EU IT systems that process sensitive data for the purposes of EU law: the Schengen Information System (SIS II), Eurodac, the Customs Information System (CIS) and the Visa Information System (VIS). It oversees the activities of these agencies and information systems, ensuring that data is processed properly and dealing with any difficulty in the application and interpretation of the relevant legal provisions. It ensures, in particular, that the rights of the individual are not affected by the storage, processing and use of the data held by the agencies. It also monitors the transmission of data originating from the agencies, particularly when third parties are involved.

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

Organisation and tasks differ slightly between agencies. The Joint Supervisory Board of Europol meets at least four times a year and issues public minutes (Europol 2009b). Once a year it conducts a full inspection and, where necessary, additional inspections dedicated to specific issues (Wills et al. 2011, p. 62). Eurojust's JSB meets twice a year, carries out a full inspection every two years with a follow-up visit the next year and may also make regular on-the-spot inspections (Eurojust 2009; Wills et al. 2011, pp. 62–3). Europol's Management Board appoints an independent Data Protection Officer tasked with ensuring the lawful processing of personal data, reporting annually on compliance with the Europol decision and cooperating with the Joint Supervisory Body (Europol 2009b).

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

The Visa Information System (VIS) Supervision Co-ordination Group is made up of representatives of the national VIS supervisory authorities from each Member State and the European Data Protection Supervisor. It aims to enhance cooperation between the national supervisory authorities and ensure the coordinated supervision of VIS and national systems. It assists the supervisory authorities in carrying out audits and inspections. It also examines problems with the exercise of independent supervision, especially regarding the rights of data subjects (VIS 2013).

In recent years Eurodac, which processes alpha-numerical and biometric data for EU asylum policy purposes, has developed coordinated supervision engaging national entities, data protection authorities (DPAs), and the European Data Protection Supervisor (EDPS). While each DPA monitors the collection and use of data in their own country, the EDPS monitors the activities of Eurodac's central unit to ensure respect for the rights of data subjects (Eurodac 2009).

Another layer of vertical oversight involves national parliaments. The national legislatures exercise control and oversight of domestic intelligence services and their foreign linkages. National parliaments remain at the heart of democratic control over the intelligence sector in Member States (Herranz-Surrallés 2014, p. 9). Article 88 TFEU provides that Europol's activities, including the collection, storage, processing, analysis and exchange of information, must be scrutinised by national parliaments (see Abazi 2014, pp. 1129–30). Likewise Eurojust, in conformity with Article 85 TFEU, is obliged to involve national parliaments in the evaluation of its activities. However, the treaty stipulates that detailed provisions should be adopted by the European Parliament and the Council. Given the sensitivity and complexity of this matter, no regulation has been adopted for the time being. In practice, national parliaments do not enjoy any significant supervisory power over Europol and Eurojust.

Horizontal Intelligence Oversight in the EU

The horizontal dimension seems appropriate for an extensive institutional network where entities making up the complex organisational structure are closely connected. In the case of EU intelligence oversight, the institutional network is not well developed and the relationships between respective entities are not balanced, because the Council of the EU and the European Council are principally embedded in vertical governmental structures which have quite limited monitoring roles at the EU level.

The European Parliament, with its strong democratic legitimacy, appears to be the appropriate institution to deal with controversial and demanding issues of transparency, control and oversight. The Court of Justice of the EU is limited by the provisions of the EU treaties and is generally excluded from rulings on intelligence cooperation in the Union. A number of specialised bodies involved in the monitoring of the handling of sensitive information, especially personal data, only have a marginal impact on the European intelligence community; their oversight competences are nevertheless briefly presented here.

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

The European Parliament occupies a prominent place in the EU system of horizontal oversight, especially following the Lisbon treaty reform. Its oversight competences have been widened formally and strengthened in practice, although they still lack sharpness and are constrained by existing regulations on access to classified information. In the realms of diplomacy, security and defence it is principally confined to general supervisory powers over the CFSP and the CSDP and to budgetary powers. Its access to classified information, and hence influence on the decision-making process, is limited. It is not concerned with military operations and budgetary expenditure and is limited to a tiny group of five MEPs—the ‘Gang of Five’ (Curtin 2013, p. 445)—who have to meet stringent criteria of access to classified information (Rosén 2014, pp. 5–6). The 2002 inter-institutional agreement between the European Parliament and the Council established procedures on access by the European Parliament to sensitive information in the field of security and defence policy (European Parliament and the Council of the EU 2002). A new arrangement, drafted in 2012 but still not approved by mid-2015, does not change the essential provisions although the scope of the arrangement is extended to the CFSP and EEAS appears as a party to it. Access to classified information is still severely restricted but not limited in number (Council of the EU 2012c).

The European Parliament has the right to be consulted and kept regularly informed of developments in CSDP matters.

In the comparative historical perspective, parliamentary oversight was seen as an underdeveloped area hampered by 'the logic of intergovernmentalism favouring the executives over the legislatives' (Puntscher Riekmann 2008, p. 32). However, while the European Parliament has gained more influence over agencies involved in the EU criminal intelligence hub, such as Europol and Eurojust, this new capacity is not yet fully effective. Article 88 of the TFEU stipulates that Europol's activities, including the collection, storage, processing, analysis and exchange of information, in particular that forwarded by the authorities of Member States or third countries or bodies, must be scrutinised by the European Parliament. Similarly, according to Article 85 TFEU, the evaluation of Eurojust activities will involve the European Parliament. In 2010 the European Parliament published a communication on Europol scrutiny (European Commission 2010b). In 2013 the European Commission presented proposals for new regulations reconstituting both agencies. Interestingly, detailed provisions concerning parliamentary scrutiny of the two agencies differ substantially, highlighting the essential distinction between 'evaluation' (Eurojust) (European Commission 2013a) and 'scrutiny' (Europol) (European Commission 2013b). According to these proposals, both agencies are subject to general evaluation requirements including the appearance of the heads of the agencies and chairpersons of the Management Boards before the European Parliament (taking into account the obligation to observe discretion and confidentiality), delivery of reports, studies and evaluations and information about administrative arrangements concluded by the agencies with third parties. In the case of Europol, scrutiny includes the European Parliament's right of access to 'sensitive non-classified information processed through or by Europol' as well as European Union classified information (Council of the EU 2014c).

Unlike Europol and Eurojust, Frontex is not explicitly mentioned in the Treaty on the Functioning of the European Union in the context of either scrutiny or evaluation of its activities. The European Parliament, then, executes general oversight but this is deemed insufficient for the effective supervision of the management of sensitive data, particularly for the purposes of risk analysis, threat assessment, situational and pre-frontier intelligence pictures. This relates particularly to the controversy over processing the personal data of certain migrant groups (returnees, 'facilitators', suspected human traffickers), where Frontex used to apply the secrecy rule (Carrera 2007, p. 14).

In response to this accountability deficit, in 2012 Frontex established a Consultative Forum to improve mechanisms for monitoring respect for fundamental rights in all the agency's activities. The Forum brought together officials from EU agencies, such as the European Asylum Support Office and the Fundamental Rights Agency, international intergovernmental humanitarian organisations (the United Nations High Commissioner for Refugees, OSCE, Council of Europe) and representatives of civil society organisations active in the field of human rights, privacy and migration (such as Amnesty International, the European Council for Refugees and Exiles, the International Commission of Jurists, the Jesuit Refugee Service Europe, Red Cross Europe and others) (Frontex 2015a). In its first two years, the Consultative Forum on many occasions raised issues of personal data, risk analyses and the methodology employed by Frontex's Risk Analysis Unit (Frontex 2014, 2015b).

The European Parliament also has an important competence in the sphere of the EU's external relations. According to Article 218 of the TFEU, its consent is required for the conclusion of international agreements that cover fields to which ordinary legislative procedure applies. Therefore, the European Parliament exercises control over the international commitments negotiated by the Commission and made by the Council. Any international agreement adopted by the EU with regard to information exchange and data sharing must be approved by the European Parliament, which has shown particular determination and engagement in the cases of PNR, SWIFT and the data protection Umbrella Agreement. EU institutions face a serious dilemma when evaluating established working arrangements from the perspective of fundamental rights and civil liberties, namely privacy, personal data protection and remedies. The European Parliament has been particularly determined to prevent EU citizens from any possible misuse or abuse of their privacy for the sake of security measures adopted during the 'war on terror'.

The European Parliament garnered considerable experience during a special inquiry into the so-called Echelon affair. Echelon was a secret global electronic surveillance system set up in the 1970s and operated by the US National Security Agency. It used communication intelligence (COMINT) techniques and equipment to intercept satellite connections, and sorted phone calls, telex, telegraph and computer signals. It was targeted at governments, organisations, companies and individuals. The interception of secret information on European companies, revealed by the press in the late 1990s and interpreted as industrial espionage, sparked widespread outrage in European societies and provoked anti-American sentiments. In a report published in July 2001 by a committee of enquiry, the practice of espionage was confirmed and the European Parliament called on Member States to adopt legislation providing for the appropriate protection of privacy and confidentiality of business communications (European Parliament 2001, 2002, 2014a). After 9/11, the strategic partnership between the EU and the US in the 'war on terror' marginalised the controversies over the Echelon system and even strengthened mutual cooperation in communication and signals intelligence. Despite the European Parliament's call to establish a European platform for representatives of national monitoring bodies to scrutinise the consistency of national laws with European law, little progress has been made.

The European Parliament's oversight also includes activities of individual members (MEPs), not only during debates, but also in the form of questions addressed to EU institutions that have vertical oversight and administrative control over EU intelligence bodies. These questions not only sought explanations for certain aspects of EU intelligence cooperation but also explored the sensitivity of information possessed by EU institutions, mainly the Council and the Commission, and the framework of its availability under applicable EU law.

Judicial control over EU agencies and bodies involved in intelligence-led activities has remained a source of concern, mostly due to certain exceptions and the exclusion of operational activities from Court of Justice control (Gless 2002; Wagner 2006; De Moor and Vermeulen 2010). According to the relevant provisions of the Lisbon treaty (Article 275 TFEU), the Court has no jurisdiction in matters of common security and defence policy (Keukeleire and Delreux 2014, pp. 89–90; Hillion 2014). In addition, the Court is not authorised to review the validity or proportionality of operations carried out by the police or other law-enforcement services of a Member State, nor the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security (Article 276 TFEU).

Conclusions

The EU strategic intelligence community generates mixed responses to questions of oversight and accountability. Müller-Wille observed, as early as the mid-2000s, that 'The main deficits in terms of democratic accountability of the European intelligence community are located at the national level. This is where the collection of intelligence takes place, the main risk of abuse of state powers lies, and the greatest threats are posed to civil liberties' (Müller-Wille 2006, p. 125). Indeed, the principle of originator control is the critical determinant of intelligence oversight in the EU, hampering efforts to strengthen the independent control and supervision of information management and intelligence sharing in the EU security fields (Walsh 2006, p. 635; Abazi 2014, p. 1122).

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

On the other hand, robust intelligence cooperation requires an adequate level of discretion, which can limit the oversight capacities of transnational bodies, without necessarily curbing the accountability of institutions involved in intelligence sharing. As Curtin, Mair and Papadopoulos argue (2010, pp. 936–7), openness has not always been regarded as an obvious element of government. The oversight functions performed by the European Parliament emphasise the transparency of EU agencies and access to all available information concerning intelligence cooperation at the EU level. Abazi (2014, p. 1132) rightly observes that 'The new oversight role of the European Parliament is multifaceted and highly dependent on receiving information, either in the form of reports or through direct questions and statements'. However, the European Parliament has been consistently separated from the sensitive information and pre-processed intelligence delivered by intelligence agencies from Member States. Governments still have plenty of room to manoeuvre when it comes to formal oversight and accountability procedures. Their strong position vis-à-vis EU oversight institutions and bodies means that transnational intelligence cooperation and information exchange can barely escape existing national mechanisms of control and evaluation.

The European intelligence community is a network structure operating at the strategic level of information exchange and knowledge management. Evaluation and assessment of the scope and content of intelligence production is a joint undertaking by EU agencies and units and respective national services. Institutional oversight includes a set of measures, procedures and mechanisms generated at the intersection of separate ambits of intelligence management and tradecraft, practised in the EU by its agencies and Member States. As a result, the oversight and accountability of the EU intelligence community are subject to disaggregated policy arrangements—an inherent feature of the EU intelligence community as a distorted epistemic community.

Bibliography

Abazi, V. (2014). The future of Europol's parliamentary oversight: A great leap forward? *German Law Journal, 15*(6), 1121–1143.

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

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

Bigo, D. et al. (2015). *National security and secret evidence in legislation and before the courts: Exploring the challenges.* CEPS Paper in Liberty and Security No. 78. Brussels: CEPS.

Bono, G. (2006). Challenges of democratic oversight of EU security policies. *European Security, 15*(4), 431–449.

Born, H., Leigh, I., & Wills, A. (2015). *Making international intelligence cooperation accountable.* Geneva: EOS-DCAF.

Bovens, M. (2007a). New forms of accountability and EU-governance. *Comparative European Politics, 5*(1), 104–120.

Bovens, M. (2010). Two concepts of accountability: Accountability as a virtue and as a mechanism. *West European Politics, 33*(5), 946–967.

Bovens, M., Curtin, D., & t'Hart, P. (2010). Studying the real world of EU accountability: Framework and design. In M. Bovens, D. Curtin, & P. t'Hart (Eds.), *The real world of EU accountability. What deficit?* Oxford: Oxford University Press.

BVerfG (2009). Lisbon Case, cases 2 BvE 2/08 and others from 30 June 2009, para. 289. At http://www.bundesverfassungsgericht.de/entscheidungen/es20090630_2bve000208en.html. Accessed 10 Mar 2015.

Caparini, M. (2007). Controlling and overseeing intelligence services in democratic states. In H. Born & M. Caparini (Eds.), *Democratic control of intelligence services: Containing rogue elephants.* Aldershot/Burlington: Ashgate.

Carrera, S. (2007). *The EU border management strategy. FRONTEX and the challenges of irregular immigration in the Canary Islands.* CEPS Working Document No. 261. Brussels: CEPS.

Clerix, K. (2014). Ilkka Salmi, the EU's spymaster. *Mondiaal Nieuws*, 4 March. At http://www.mo.be/en/interview/ilkka-salmi-eu-s-007. Accessed 10 June 2014.

Council of the EU (1995). La Gomera declaration. At http://www.europarl.europa.eu/summits/mad2_en.htm#annex3. Accessed 17 Feb 2009.

Council of the EU (2002, March 6). Council decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime. *Official Journal of the European Communities, L 63.*

Council of the EU (2012c, October 23). Access by the European Parliament to classified information in the area of the Common Foreign and Security Policy, doc. 15343/12Brussels.

Council of the EU (2014c, May 28). Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA (First reading)—General Approach, doc. 10033/14, Brussels.

Council of the EU (2015, July 14). Renewed European Union internal security strategy implementation paper, doc. 10854/15, Brussels.

Curtin, D. (2013). Official secrets and the negotiation of international agreements: Is the EU executive unbound? *Common Market Law Review, 50*(2), 423–458.

Curtin, D., Mair, P., & Papadopoulos, Y. (2010). Positioning accountability in European governance: An introduction. *West European Politics, 33*(5), 929–945.

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

De Moor, A., & Vermeulen, G. (2011). Europol and Eurojust. In A. Wills et al. (Eds.), *Parliamentary oversight of security and intelligence agencies in the European Union*. Brussels: European Parliament.

Erskine, T. (2004). 'As rays of light to the human soul'? Moral agents and intelligence gathering. *Intelligence and National Security, 19*(2), 359–381.

Eurodac (2009). Eurodac supervision coordination group second inspection report—Executive summary. At https://secur0065.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Eurodac/09-06-24_Eurodac_report2_summary_EN.pdf. Accessed 16 May 2015.

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

European Commission (2010b, December 17). Communication from the Commission to the European Parliament and the Council on the procedures for the scrutiny of Europol's activities by the European Parliament, together with national Parliaments, doc. COM(2010) 776 final, Brussels.

European Commission (2013a, July 17). Proposal for a regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust), doc. COM(2013) 535 final, Brussels.

European Commission (2013b, March 27). Proposal for a regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, doc. COM(2013) 173 final, Brussels.

European Parliament (2001, July 11). Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), doc. A5-0264/2001 FINAL, Strasbourg.

European Parliament (2002, March 21). European Parliament resolution on the existence of a global system for the interception of private and commercial communications (Echelon interception system). *Official Journal of the European Communities, C 72 E.*

European Parliament (2014a). *The ECHELON affair. The European Parliament and the global interception system. Study.* Luxembourg: European Parliamentary Research Service.

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

Frontex (2014). Frontex consultative forum on fundamental rights. Annual Report 2013. At http://frontex.europa.eu/assets/Partners/Consultative_Forum_files/Frontex_Consultative_Forum_annual_report_2013.pdf. Accessed 5 Sept 2015.

Frontex (2015a). Frontex Consultative Forum on fundamental rights background note for the public call for applications. At http://frontex.europa.eu/assets/Attachments_News/CF_call_documents/Background_doc_for_public_call_FINAL.pdf. Accessed 1 July 2015 .

Frontex (2015b). Frontex consultative forum on fundamental rights. Second Annual Report 2014. At http://frontex.europa.eu/assets/Partners/Consultative_Forum_files/Frontex_Consultative_Forum_annual_report_2014.pdf. Accessed 5 Sept 2015.

Gill, P., & Phythian, M. (2012). *Intelligence in an insecure world* (2nd ed.). Cambridge: Polity Press.

Gless, S. (2002). What kind of judicial control do the new protagonists need?: The accountability of the European Police Office (Europol). In G. de Kerchove & A. Weyemberg (Eds.), *L'espace pénal européen: enjeux et perspectives*. Bruxelles: Editions de l'Université de Bruxelles.

Grant, R. W., & Keohane, R. O. (2005). Accountability and abuses of power in world politics. *American Political Science Review, 99*(1), 29–44.

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

Herranz-Surrallés, A. (2014) *Parliamentary oversight of EU foreign and security policy: Moving beyond the patchwork?*. ISPI Analysis No. 230. At http://www.ispionline.it/sites/default/files/pubblicazioni/analysis_230_2013.pdf. Accessed 15 Mar 2015.

Hillion, Ch. (2014). A powerless Court? The European Court of Justice and the common foreign and security policy. In M. Cremona & A. Thies (Eds.) (2014), *The European Court of Justice and external relations law. Constitutional challenges*. Oxford/Portland: Hart Publishing.

Keohane, R. O. (2006). Accountability in world politics. *Scandinavian Political Studies, 29*(2), 75–87.

Keukeleire, S., & Delreux, T. (2014). *The foreign policy of the European Union*. Basingstoke/New York: Palgrave Macmillan.

Leigh, I. (2007). The accountability of security and intelligence agencies. In L.K. Johnson (Ed.), *Handbook of intelligence studies*. London/New York: Routledge.

Leigh, I. (2011). Accountability and intelligence cooperation: Framing the issue. In H. Born, I. Leigh, & A. Willis (Eds.), *International intelligence cooperation and accountability*. Abingdon/New York: Routledge.

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

Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society, 1*(3), 331–355.

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

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

Pastor, R. A. (1999). The third dimension of accountability: The international community in national elections. In A. Schedler, L. Diamond, & M. F. Plattner (Eds.), *The self-restraining state. Power and accountability in new democracies*. Boulder/London: Lynne Rienner Publishers.

Puntscher Riekmann, S. (2008). Security, freedom and accountability: Europol and Frontex. In E. Guild & F. Geyer (Eds.), *Security versus justice? Police and judicial cooperation in the European Union*. Aldershot/Burlington: Ashgate.

Rosén, G. (2014). *Secrecy versus accountability parliamentary scrutiny of EU Security and Defence Policy*. ARENA Working Paper 1/14. At http://www.sv.uio.no/arena/english/research/publications/arena-publications/working-papers/working-papers2014/wp1-14.pdf. Accessed 15 Mar 2015.

Trechsel, A. H. (2010). Reflexive accountability and direct democracy. *West European Politics, 33*(5), 1050–1064.

Van Buuren, J. (2013). From oversight to undersight: The internationalization of intelligence. *Security and Human Rights, 24*(3-4), 239–252.

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

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

Waldrauch, H. (1998). *Institutionalizing horizontal accountability. A conference report*. Political Science Series No. 55. Vienna: Institute for Advanced Studies.

Walsh, J. I. (2006). Intelligence-sharing in the European Union: Institutions are not enough. *Journal of Common Market Studies, 44*(3), 625–643.

Wetzling, Th. (2009). European intelligence cooperation and accountability. In: S. Gustavsson, Ch. Karlsson, & Th. Persson (Eds.), *The illusion of accountability in the European Union*. London/New York: Routledge.

Wills, A., et al. (2011). *Parliamentary oversight of security and intelligence agencies in the European Union*. Brussels: European Parliament.

CHAPTER 11

Conclusions: The Maturing EU Intelligence Community

The rich scholarship in intelligence studies is based on the assumption that national security is the domain of the state authorities responsible for the organisation and functioning of the intelligence services. This state-centric perspective stems from a direct link between intelligence, and the protection of state sovereignty and national interests. It is also the result of the particular position of intelligence services within legal and political systems. The purpose of intelligence is to obtain information and data relating to the fundamental interests of the state, especially in the field of national and international security, and process them into analytical material used by decision makers. Intelligence activities are conducted by relevant state bodies, but increasing bilateral and multilateral international cooperation can be seen in the acquisition, processing and sharing of intelligence products. International structures have emerged to enable communication between national intelligence services and to pool common resources to improve intelligence production.

EU intelligence cooperation has been evolving towards a phronetic community based on complex networks connecting security actors who use practical knowledge to activate, develop and maintain intelligence security. This community uses the networked architecture of information exchange and intelligence sharing between EU agencies and its Member States, and the functional isomorphic patterns developed by some Member States.

A. Gruszczak, *Intelligence Security in the European Union*,
DOI 10.1057/978-1-137-45512-3_11

The Archaeology of EU Intelligence Cooperation: Going to the Sources

The idea of an intelligence community in democratic Europe began to form in the minds of politicians and experts during the accelerated political and security integration of the early 1990s. The EU's economic integration, and military and law-enforcement security cooperation (the second and third pillars) led to questions about the Union's real ability to guarantee the safety of its citizens and provide continued and adequate support for the national security policies of Member States.

Early debates on intelligence security in the EU were rather disappointing, marked by inconsistency, divisiveness and sovereignty-driven arguments. Governments of Member States preferred informal initiatives to formal regulations, narrow coalitions to EU-wide consensual arrangements, and ad hoc undertakings to institutional solutions. The hybrid nature of the European Union facilitated the fuzzy logic of security cooperation and the interconnections within bilateral and multilateral collaboration among Member States determined by EU legal and institutional competences. The chances of developing and adopting a comprehensive approach to the organisation and functioning of intelligence cooperation in the EU were slight. Alessandro Politi (1998b, p. 16) found, as early as 1998, that 'a European intelligence policy or community need not be complex or highly formalized'. The political imperative to develop a common security and defence policy and to strengthen internal security cooperation among law-enforcement services had implications for intelligence capabilities and solutions. Any military operation involving EU forces required proper and effective planning, reconnaissance, situational awareness and information management. As a part of multinational forces the EU could rely on external intelligence support, as in the case of the Balkans in the 1990s where NATO provided the necessary information and intelligence input. However, the ambition of the EU to acquire a more independent role and to increase its capabilities for autonomous military operations in the context of the newly evolving post-Cold War global security environment induced Member States at the turn of the century to agree on institutional and structural changes.

According to Dorn (2008, p. 167) the need for additional security measures in the face of increasing security threats, the damage done by serious and organised crime, the close links between intra- and non-EU criminal networks and the fuzzy boundaries between the internal and external dimensions of security was the main driver for the development of intelligence cooperation within the EU political and institutional framework.

The positive element of the European integration process was reflected in the functional spill-over in the area of the free movement of persons identified with the creation of the Schengen zone. Member States were obliged to put more emphasis on cross-border cooperation in preventing and fighting crime as well as reinforcing their frontiers and modernising border infrastructure, especially in its external sections with non-EU countries. The amount of information and data exchanged between police officers, border guards and intelligence services of the Member States was growing in volume and relevance, overcoming some of the latters' reservations about further cooperation in the intelligence field. In a follow-up to the 1999 summit meetings, EU heads of state and government increasingly highlighted intelligence collection and analysis capabilities as a necessary component of the ESDP (Villadsen 2000, p. 81), foreseeing the possibility of achieving the relative operational autonomy that would allow the implementation of the Petersberg tasks without directly involving NATO. To this end, future European forces would have to build capacities compatible with the requirements of command, control and intelligence in order to perform on the international stage as legitimate actors ready for effective crisis response and post-conflict stabilisation.

In the late 1990s Alessandro Politi had already identified opportunities for close intelligence cooperation. He wrote: 'Since intelligence objectives and methods are not determined by some abstract political requirement but are driven by an individual intelligence service that is trying to anticipate and satisfy the needs of its political masters, a European intelligence policy need not be a highly formalized and institutionalized affair. It should be perceived and practised rather as an alternative culture which may shape the collective behaviour of the services concerned' (Politi 1998b, p. 8). Klaus Becher, a senior research fellow at Stiftung Wissenschaft und Politik, noticed at that time that 'Future developments in intelligence in Europe are going to be shaped [...] by externally imposed political expectations. In return for continued funding, European governments will demand that intelligence supports them efficiently in their effort to master today's complicated political agenda in a continent that is both widening and deepening its economic and political integration, and having to face up to broader responsibilities in a social and economic environment of rapid change on a global scale' (Becher 1998, p. 37).

From its beginnings, intelligence cooperation in the EU has encountered numerous problems due to the low level of trust between competent authorities of Member States, poorly developed communication networks and differences in techniques and methods of intelligence. Nevertheless, it received a strong impetus at the beginning of the 2000s in response to the proliferation of threats and the emergence of global challenges and risks.

Networks over Hierarchies

The 'soft' approach to intelligence cooperation in the EU was conducive to the emergence of functional-institutional 'focal points' where relevant EU agencies and units organised information exchange and intelligence production within the frameworks determined by EU security objectives and Member States' national interests. The complex network of intelligence hubs established in different areas of European security integration has significant advantages in terms of information workflow, multi-source analysis, strategic outlook and the ability to generate synergetic connections. However, the possibility of setting up a central EU intelligence unit arose in crisis situations (after the 9/11 and 3/11 terrorist attacks, following disclosure of US secret intelligence activities in EU Member States), acting as a wake-up call for Member States which were neglecting intelligence sharing with EU agencies and occasioning security gaps in EU policies.

Interestingly the concept of a European intelligence agency had surfaced already in the early 1990s, coinciding with the grand reform of the European integration edifice. Jaap Donath, a Dutch scholar investigating the directions of security integration in the early 1990s, asserted that 'The European Community (EC) needs a strategic intelligence organization comparable to the Central Intelligence Agency. […] Its most important task would be the analysis of overtly gathered information and preparing it for use by the policymakers. […] For the long-term prospect the ECIO [European Community Intelligence Organisation] should become an organization which recruits and trains its own personnel for all the information gathering' (Donath 1993, p. 16).

The idea of an EU intelligence agency also appeared several times on the surface of Brussels' political life. In the post-Lisbon legal and institutional setting, it reappeared in public debate in the aftermath of the so-called PRISM affair (Bigo et al. 2013). Vivienne Reding, Vice-President of the European Commission and Commissioner for Justice and Fundamental

Rights, endorsed the idea of establishing a European intelligence agency by 2020. In an interview for the Greek daily *Naftemporiki* the Commissioner severely criticised the surveillance of EU institutions and Member States that was carried out by the US National Security Agency. She stressed the necessity of having a single and coherent set of data protection rules in the EU in relation to the United States and other countries which develop and strengthen cooperation and partnership with the Union in political, economic and security-related matters. She supported a Franco-German initiative presented to the European Council for bilateral talks with the USA to find an understanding on mutual relations in the field of intelligence cooperation (European Council 2013). She said: 'What we need is to strengthen Europe in th[e intelligence] field, so we can level the playing field with our US partners, I would therefore wish to use this occasion to negotiate an agreement on stronger secret service cooperation among the EU Member States – so that we can speak with a strong common voice to the US. The NSA needs a counterweight. My long-term proposal would therefore be to set up a European Intelligence Service by 2020' (Reding 2013).

Commissioner Reding's idea of a European intelligence service was preceded by questions from a Dutch MEP to the Commission concerning 'the creation of a single intelligence service', understood and interpreted as 'an attempt to set up a European equivalent of the American CIA' (European Parliament 2013b, p. 581). In response to this question, HR/VP Ashton firmly stated that 'There are no plans to create a "European" intelligence service'. Interestingly, Baroness Ashton indicated that 'any initiative in this field would be governed by Title V of the Treaty on the Functioning of the European Union which already contains a number of procedural and substantive provisions with regard to Member States and Union prerogatives in this regard' (European Parliament 2013b, p. 581). The Council recalled that 'Article 73[1] of the Treaty on the Functioning of the European Union leaves it up to the Member States to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between national security Departments' (European Parliament 2010b).

Given that Title V of the TFEU contains provisions in the area of freedom, security and justice, Ashton's answer suggested that intelligence cooperation might develop in the field of policing and criminal justice. A Dutch MEP, Laurence J.A.J. Stassen, asked for clarification of Commissioner Reding's suggestions about a future EU intelligence agency with regard to earlier assurances that the EU had no plans to establish a secret service (European Parliament 2014b, p. 430). Vivienne Reding affirmed that 'There are currently no plans to establish a European intelligence service'. She qualified her earlier statements, arguing that they referred 'to the need to speak with a strong common voice to the US on matters related to national security'. Commissioner Reding advanced the following thesis: 'The establishment of a European intelligence service would require a change in the Treaties.' She referred to the provision of Article 4.2. TEU, which contained a general national security clause (European Parliament 2014b, p. 430). In fact, such a standpoint has to be referred to an earlier interpretation made by the Council in answer to a question from two MEPs concerning the CIA secret flights in Europe (European Parliament 2013c, p. 109). The Council invoked the provision of Article 4.2. TEU and decisively stated that 'the work of Member States' intelligence agencies for national security matters remains the sole responsibility of Member States'. In a similar vein, Ilkka Salmi, the director of EU INTCEN, argued that the setting up of an EU intelligence agency would entail treaty reform, given that the binding general provisions of the TEU clearly stated that national security fell within the competence of Member States. Moreover, he raised a practical question concerning real value added to the ongoing intelligence collaboration between Member States which is, in his view, 'a very intensive cooperation in European intelligence and security services anyway' (Clerix 2014).

The latter remark is particularly significant when discussing the strengths and weaknesses of the EU strategic intelligence community. Evidently, the EU intelligence community unites, to put it figuratively following Cogan (2004), gatherers, not hunters. The model that has been constructed since the late 1990s has been framed by network arrangements and multidimensional communication channels interconnecting EU and national stakeholders. It was thoroughly deliberated on by Member States which sought a functional arrangement for a comprehensive assessment and analysis of the growing amount of information and intelligence concerning not only their national security, but also EU-wide security objectives and concerns. In practical terms, the network architecture enables a controlled information exchange and gives intelligence support for strategic assessments and risk analyses prepared either by EU agencies or national intelligence services. It should be pointed out that the network architecture protects national security interests and meets the intelligence requirements of Member States. Shapcott (2011, p. 123) remarked that 'The EU model separates collection, assessment and policy. Collection is generally the business of MS and their intelligence services, with a small portion of this harvest being made available to the EU. In the EU, assessment stands apart from policy, which is for a wider circle.'

The arguments presented above justify the conclusion that the networked configuration of interconnected intelligence hubs in the EU successfully compensates the lack of a centralised hierarchical structure of intelligence sharing. The primacy of networks over hierarchies is a direct effect of the national interests and security clauses which underpin Member States' policies, and are respected by EU law. The horizontal dimension of EU intelligence cooperation makes room for specific policies and actions which provide the EU strategic intelligence community with strong national legitimacy and at the same time keep Member States' sovereign interests intact.

Towards a Phronetic Intelligence Community

The EU intelligence community does not resemble a state-centric intelligence community. Its legal and structural framework fits, rather, the model of distorted epistemic community. Its heterogenous architecture is structured by hubs determining specific modes and methods of intelligence proper for a given field of security. The communication and intelligence flow between the hubs is basically limited. Nevertheless, intelligence products originating in single hubs can be shared with other stakeholders in EU security policy, subject to political acquiescence and the formal consent of Member States. The EU's distorted epistemic community enables, as a system of systems, regular information workflow and occasional intelligence sharing, yet it does not respond effectively to emerging complex threats and risks demanding a comprehensive approach to knowledge management. This model of intelligence community suffers certain information deficits, organisational faults and decision-making bottlenecks inherent in supranational arrangements striving for the maximisation of added value to the information pool and analytical coordination. It does not preclude the absorbing of certain elements of national intelligence tradecraft and hierarchical organisation but it cannot follow isomorphic patterns typical for a vertically structured intelligence architecture contingent on the sovereign authority of the founding states.

William Shapcott (2011, p. 118) asserted that 'the EU itself has no intelligence agency of its own, no secret intelligence assets, and that therefore many of the features of the traditional intelligence cycle are absent or only present in a very distorted form'. This statement is another brick in the wall of misunderstanding that has surrounded EU efforts to establish and develop an intelligence community *sui generis*. As argued above, the EU intelligence community in the making has not been following the beaten track of national intelligence communities functioning in numerous Member States as well as outside the Union. Member States, along with relevant EU institutions and agencies, pretend to build a transnational intelligence community on the grounds of the effective rendering of time-sensitive intelligence, sharing of best practices and analytical products and supporting decision-making processes both at the EU level and in Member States.

So, I can agree with Mai'a Davis Cross that Member States have reached a general consensus as to the building of a trans-governmental intelligence network at the EU level. However, it is hard to accept her argument that 'the achievement of closer cooperation in this sensitive area no longer depends on member states' willingness to overcome sovereignty concerns and trust issues' (Davis Cross 2013c, p. 395). Intelligence, as I tried to demonstrate in Chap. 2, is the process of knowledge production serving legitimate decision makers in the areas of national security, public order and international co-existence. The EU strategic intelligence community, conceived as a distorted epistemic community, presumes the linking of open and secret sources of information in transversal and heterogenous frameworks, strongly determined by sovereign rights and national interests. One has to bear in mind that Member States are still the 'Masters of the European Treaties', and that security is that realm of European integration which is underpinned, and permeated, by national security priorities, objectives and resources. Nevertheless, the primacy of Member States is questionable as far as the strategic dimension of intelligence cooperation is concerned. This is due to the fact that the patterns of isomorphism enforced by state actors tend to weaken transnational ties, limit network agility and reduce information flows as well as intelligence output. It is hard to find a simple solution to this dilemma because of the transversal dependencies underpinning EU intelligence cooperation.

I find the rationale for maintaining and developing the EU strategic intelligence community in the conception of knowledge as practical wisdom, or—borrowing from Aristotle (1886, p. 187)—phronesis, to be prudent. Phronesis is practical wisdom; it can be equated with the ability to produce opinions, a proper understanding of issues, the power of foresight, and clear-sightedness. Knowledge in the world of intelligence is more in the nature of practical wisdom than a formal result of the application of an exact formula extracted from optimum-based large-scale algorithmic data mining. Intelligence in its practical meaning is directly related to decision- and policy making in a strategic context. Recalling Johnson's and Wirtz's understanding of strategic intelligence, it is worth emphasising that this kind of intelligence 'provides warning of immediate threats to vital national security interests and assesses long-term trends of interest to senior government officials' (Johnson and Wirtz 2004, p. 2).

Everyday intelligence activity is focused on the provision of intelligence products and analytical inputs for decision making. It has to contain practical knowledge about a whole range of facts (events, developments, processes) which are decisive for the effectiveness of decisions and actions. The phronetic approach to intelligence involves prudent, multi- and counterfactual thinking engaging intellectual capacities and organisational structures. Flyvbjerg (2008, p. 154) points out that phronesis 'goes beyond analytical, scientific knowledge (episteme) […] and technical knowledge or know how (techne) and it involves judgements and decisions […].' This is particularly important in intelligence activities given the need, which is often quite desperate, for a single end product which determines the choice of the final solution to a security dilemma. Phronetic intelligence, then, has to combine analytical materials with technical knowledge and add the specific practical wisdom that is an outcome of individual abilities, talents and skills as well as common sense and experience.

A phronetic intelligence community needs to be based on intelligent multi-centric inter-personal and inter-institutional networks connecting individuals who are capable and willing to establish synergies that enable a streamlined transfer of elements ('particles') of practical wisdom activating, supporting or enhancing the intelligence cycle on various stages and in different locations. Shifting to the state level, one has to bear in mind that synergetic connections between phronetic-prone individuals emerge in the given institutional, often highly politicised environment inhabited by state actors and governmental entities. Networks that make up a phronetic intelligence community are state-dependent, and it is the government which controls, steers and administers to these networks (often with no feedback from legislative power). For this reason, practical wisdom can be delivered on behalf of the state authorities and put into the sphere of internal security or foreign policy demarcated in accordance with the capacities of governments and the opportunities to deliver provided by international institutions or supranational agencies. ‘The virtue of prudence’ of the phronetic intelligence community is manifested in synergetic linkages within the network structure of information management for the purpose of intelligence analysis. These linkages are created with the consent of the participating states and within the logic of trans-governmental networks connecting institutions and agencies aware of the limitations forced on them by states. As a result, intelligence community stakeholders focus their efforts on practical national security objectives, yet at the same time are fully dedicated to collaborative ventures in the field of collecting, processing and analysing information and data because the outcomes of international intelligence cooperation facilitate decision-making processes in the national security dimension. As a result, the patterns and mechanisms of intelligence cycles in individual countries do not interfere with the procedures applicable at the international level, and these—on the basis of the feedback system—rationalise the practical needs arising from the implementation of regional or global security policy.

The phronetic perspective on the EU intelligence community highlights certain opportunities arising from the diversity and multiplicity of agents and structures embedded in the EU’s legal and institutional construction. The flexibility of the network architecture, the horizontal dimension of co-operative mechanisms and flattened connections between the governmental and supranational dimensions of cooperation and integration, offer more opportunities for sharing and intermediation than the multicentric organisation of the distorted intelligence community. The evident weakness of this model consists in its large-scale diffusion of information and the difficulties of managing such an overwhelming amount of data through the application of relatively scarce technical, financial and human resources. In some cases limits and shortcomings provide incentives for the establishment of cooperative networks which can deliver diverse information and data extracted from dispersed sources belonging both in EU Member States’ sovereign competences and state control and in non-EU, government, public or private entities that are often cooperating with the EU on a purely commercial basis. The quality of the intelligence products made on such soft grounds can be questionable and problematic. However, the EU’s output at the stage of collating, comparing, filtering, analysing and processing information can bring added value to intelligence production thanks to the synergetic collaborative patterns and procedures established by the EU in concordance with formal norms and rules.

Studying intelligence cooperation in the EU seems to be quite a demanding task. The two predominant perspectives—the epistemic and the phronetic—correspond with each other, rather than tending to integration or fusion. They reflect general theoretical problems of studying European integration and comparing the dominant approaches applied to general or sectoral processes of integration and cooperation. Knowledge-based communities matter more and more in complex security environments. The EU's institutions and Member States must decide which elements of intelligence cooperation take priority.

Note

1. Article 73 TFEU provides that: 'It shall be open to Member States to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security' (European Union 2012, p. 74).

Bibliography

Aristotle (1886). *The Nicomachean ethics* (trans: Peters, F. H.). 3rd ed. London: Kegan Paul, Trench & Co.

Becher, K. (1998). European intelligence policy: Political and military requirements. In A. Politi (Ed.), *Towards a European intelligence policy*. Chaillot Paper No. 34. Paris: Institute for Security Studies of the WEU.

Bigo, D. et al. (2013). *Open season for data fishing on the web the challenges of the US PRISM programme for the EU*. CEPS Policy Brief no. 293. Brussels: CEPS.

Clerix, K. (2014). Ilkka Salmi, the EU's spymaster. *Mondiaal Nieuws*, 4 March. At http://www.mo.be/en/interview/ilkka-salmi-eu-s-007. Accessed 10 June 2014.

Cogan, C. (2004). Hunters not gatherers: Intelligence in the twenty-first century. *Intelligence and National Security, 19*(2), 304–321.

Davis Cross, M. K. (2013c). A European transgovernmental intelligence network and the role of IntCen. *Perspectives on European Politics and Society, 14*(3), 388–402.

Donath, J. (1993). A European Community Intelligence Organization. *Defense Intelligence Journal, 2*(1), 15–33.

Dorn, N. (2008). European strategic intelligence: How far integration? *Erasmus Law Review, 1*(5), 163–180.

European Council (2013, October 25). Statement of the heads of state or government, annex to Europea Council 24/25 October 2013 conclusions, doc. EUCO 169/13, Brussels.

European Parliament (2010b, March 8). Reply to the written question E-1352/2010 from Nick Griffin, MEP, to the Council. Subject: Intelligence and Security. At http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-1352&language=EN. Accessed 8 Mar 2013.

European Parliament (2013b, December 18). Answer given by High Representative/Vice-President Ashton on behalf of the Commission (25 April 2013) to the question for written answer E-001928/13 to the Commission (Vice-President/High Representative) from Laurence J.A.J. Stassen (NI) (22 February 2013). *Official Journal of the European Union, C 371 E.*

European Parliament (2013c, December 18). Reply (17 June 2013) to the question for written answer E-001671/13 to the Council Inês Cristina Zuber (GUE/NGL) and João Ferreira (GUE/NGL) (18 February 2013. *Official Journal of the European Union, C 371 E.*

European Parliament (2014b, March 25). Answer given by Mrs Reding on behalf of the Commission (10 January 2014) to the question for written answer E-012611/13 to the Commission Laurence J.A.J. Stassen (NI) (7 November 2013). *Official Journal of the European Union, C 86 E.*

European Union (2012). Treaty on European Union (consolidated version). *Official Journal of the European Union*, C 326, 26 October.

Flyvbjerg, B. (2008). Phronetic organizational research. In R. Thorpe & R. Holt (Eds.), *The SAGE dictionary of qualitative management research*. London: SAGE Publications.

Johnson, L. K., & Wirtz, J. J. (Eds.). (2004). *Strategic intelligence: Windows into a secret world*. Los Angeles: Roxbury.

Politi, A. (1998b). Why is a European intelligence policy necessary?. In A. Politi (Ed.), *Towards a European intelligence policy*. Chaillot Paper No. 34. Paris: Institute for Security Studies of the WEU.

Reding, V. (2013, November 1). V. Reding to naftemporiki.gr: I suggest the set up of a European Intelligence Service by 2020. *Naftemporiki*. At http://www.naftemporiki.gr/story/723823/v-reding-to-naftemporikigr-i-suggest-the-set-up-of-a-european-intelligence-service-by-2020. Accessed 3 Nov 2013.

Shapcott, W. (2011). Do they listen? Communicating warnings: An intelligence practitioner's perspective. In Ch. de Franco & Ch. O. Meyer (Eds.), *Forecasting, warning, and responding to transnational risks*. Basingstoke/New York: Palgrave Macmillan.

Villadsen, O. R. (2000). Prospects for a european common intelligence policy. *Studies in Intelligence, 44*(9), 81–95.

Index

A. Gruszczak, *Intelligence Security in the European Union*,
DOI 10.1057/978-1-137-45512-3