Counter-Terrorism Intelligence Cooperation in the European Union

Eveline R. Hertzberger

2007

European Foreign and Security Studies Policy Program
Foreword

The international community can no longer address the new challenges posed by non-state actors without adopting a unified, cooperative and supportive approach. One of the fundamental pillars in countering terrorism and governing security in the European Union (EU) involves information and intelligence sharing as this is the first step in enhancing such cooperation in the security area.

The sharing of intelligence between EU Member States seems like a simple task at first glance, but under the surface working together is not always as easy as it seems. Decision makers and agencies face legal, technical, political, cultural, organizational and even personal obstacles when sharing information. The relevant governmental and inter-governmental organizations have to overcome such obstacles and hesitation because they delay effective counter-terrorism coordination in the long-term.

To address such issues in information sharing, UNICRI has researched and published a report on ‘Counter-Terrorism Intelligence Cooperation in the European Union’. It aims to raise awareness regarding the relevant obstacles, trigger debate regarding the potential solutions and come up with innovative alternatives. The report argues for greater information flow from the national level to the international EU level. The research reveals that personal contacts and informal arrangements play a crucial role in the initiation and maintenance of intelligence cooperation relations. Counter-terrorism may therefore require a much greater investment in informal intelligence-sharing arrangements than has thus far been acknowledged.

This report does not stand alone, the Institute also works towards security governance by identifying common goals, maximizing investments, establishing a common language and creating the organizational framework needed for a permanent and sustained dialogue and information sharing. UNICRI is fully aware of the role intelligence cooperation has to play and sees this Report as another cooperative step forward in advancing security, serving justice and building peace.

Sandro Calvani
Director of UNICRI
Acknowledgement

This research was made possible by the generous contribution of Compagnia di San Paolo (Italy), Riksbankens Jubileumsfond (Sweden) and VolkswagenStiftung (Germany). I gratefully acknowledge the support of: Francesco Marelli, Francesco Cappè and Doris Buddenberg of UNICRI; Pavel Maximov for layout and graphics; Mari Kalliala of Europol; Prosecutor Stefano Dambruoso; Nicolò Russo Perez of the Compagnia di San Paolo; Christopher Langton of the International Institute for Strategic Studies; prof.mr.dr. E.R. Muller; all interviewees; all contributors; my family and friends.

Disclaimer

The opinions expressed in this publication are the sole responsibility of the author and do not necessarily reflect the views of UNICRI.

Eveline R. Hertzberger

July 2007

Turin, Italy
Abstract

Counter-terrorism intelligence sharing in the European Union is needed to provide EU decision makers with better intelligence support. Such decision makers in the Second and Third Pillar are the Council, the Commission, the Counter-terrorism Coordinator and the High Representative. Together with several EU information agencies and national intelligence and security services, they comprise the European intelligence community.

Information flow in the EU is bottom-up: information flows from national intelligence and security services, via EU information agencies, to EU decision makers in the Second and Third Pillar. However, intelligence support to EU decision makers has been insufficient. Therefore, this study aims to answer the question: what are the most important problems in counter-terrorism intelligence sharing within the European Union, and how can these problems be resolved? Better intelligence cooperation would lead to better intelligence support to EU decision makers and a substantial added value for Member States, motivating them to continue to submit intelligence to the European level.

The European intelligence community hosts four EU information agencies: the European Police Organization (Europol), the Joint Situation Center (SitCen), the Intelligence Division of the European Union Military Staff (INTDIV EUMS), and the European Union Satellite Center (EUSC). SitCen and Europol both have an explicit counter-terrorism mandate. They collect intelligence from national intelligence and security services, and analyse and process this intelligence for EU and national decision makers. Several political, cultural, technical, and organizational problems are continuing to hamper counter-terrorism intelligence cooperation in the EU.

A special focus of this study lies on the use of personal contacts and informal arrangements of information sharing to improve intelligence cooperation. It is argued that personal contacts are crucial in initiating and maintaining relationships of intelligence sharing. Investing in informal sharing arrangements and other ‘soft’ measures would be an important step for the EU to stimulate counter-terrorism intelligence cooperation.

Key words
counter-terrorism; intelligence; information sharing; Europol; SitCen; informal sharing
# Counter-Terrorism Intelligence Cooperation in the European Union

1 Introduction ............................................................................................................. 1
   1.1 Introduction ........................................................................................................ 1
   1.2 Literature review ............................................................................................ 6
   1.3 Methods ............................................................................................................ 9
   1.4 Research framework .................................................................................. 10
   1.5 Definitions .................................................................................................. 12
   1.6 Reading guidelines ................................................................................... 15

2 The Changing Security Environment of the EU ........................................ 19
   2.1 Introduction ............................................................................................... 19
   2.2 The changing security environment ....................................................... 19
   2.3 Developments in intelligence ..................................................................... 24
   2.4 The EU as a security actor ....................................................................... 29
   2.5 Conclusion .................................................................................................. 32

3 The use of intelligence to combat terrorism ............................................. 37
   3.1 Introduction ............................................................................................... 37
   3.2 Introduction to types of intelligence ....................................................... 37
   3.3 Measures to combat terrorism ................................................................. 40
   3.4 The use of intelligence to combat terrorism ........................................... 43
   3.5 Conclusion .................................................................................................. 48

4 The European intelligence community ..................................................... 51
   4.1 Introduction ............................................................................................... 51
   4.2 Description of the EU Intelligence Community ........................................ 52
   4.3 The availability principle ........................................................................... 55
   4.4 EU institutional framework for counter-terrorism ................................... 58
   4.5 National – national sharing ....................................................................... 62
   4.6 National – European sharing ................................................................... 65
   4.7 The Joint Situation Center (SitCen) ............................................................ 66
   4.8 Sharing with SitCen ................................................................................... 71
   4.9 European Police Organization (Europol) ............................................... 73
   4.10 Sharing with Europol ................................................................................ 76
   4.11 The European Union Satellite Center (EUSC) ......................................... 82
   4.12 The Intelligence Division of the EU Military Staff (INTDIV) .................. 84
Chapter 1

Introduction

1.1 Introduction

This research is funded by the European Foreign and Security Policy Studies Program. This research and training program aims at enhancing the qualification of the next generation of European intellectual leaders and policy experts. The program is a cooperation between three European foundations: Compagnia di San Paolo (Italy), Riksbankens Jubileumsfond (Sweden) and VolkswagenStiftung (Germany). The author is sincerely grateful to the Compagnia di San Paolo for their generous assistance. The research was performed at the United Nations Interregional Crime and Justice Research Institute in Turin, Italy in the period between June 2006 and June 2007.

Research Question

This study aims to fill a gap in the academic and practitioners’ research into European information sharing and the European intelligence community. Existing research focuses on mapping the European intelligence community, but does not discuss the relationships between European information agencies such as SitCen and Europol. Existing research discusses counter-terrorism and Third Pillar policy making, but disregards the role of intelligence in this policy field. Existing research focuses on intelligence cooperation in the Second Pillar of European Foreign and Security Policy, but does not discuss the role of terrorism and the interaction between the Second and Third Pillar.

1 The Second EU Pillar concerns the Common Foreign and Security Policy. The Third EU Pillar concerns Police and Judicial Cooperation in Criminal Matters. Both pillars are subject to consensus-style decision making. Decision makers in both pillars are in need of intelligence support for their policymaking.
Existing research discusses intelligence-led law enforcement, but focuses virtually solely on police cooperation and ignores national intelligence and security services.

This research aims to fill this gap. It focuses on European intelligence-led law enforcement, and more specifically on information and intelligence sharing in this process. Key terms are the use of OSINT, the importance of personal relationships and informal arrangements, better support to EU decision makers in Second and Third Pillar, the interaction between Second and Third Pillar, and the use of intelligence to combat terrorism.

This research aims to identify the gaps and provide recommendations for improved counter-terrorism intelligence cooperation in the European Union. The main research question is: what are the most important problems in counter-terrorism intelligence sharing within the European Union, and how can these problems be resolved?

The assumption is that improved intelligence cooperation will lead to two important advantages. These two arguments are the main reasons why the EU needs better counter-terrorism intelligence cooperation. Firstly, the EU will be able to provide better intelligence support to its decision makers in the Second and Third Pillar. Secondly, the EU will be able to provide added value to the intelligence process of the Member States, thereby increasing the incentives of the Member States to contribute intelligence to the EU. These two goals will be assumed throughout this study as the objectives of better counter-terrorism intelligence cooperation in the European Union. This study will prove that the EU needs better counter-terrorism intelligence support to EU decision makers, and that improved intelligence cooperation will be the most promising way to achieve this goal.

**European intelligence community**

An intelligence function is the structure which provides intelligence support to relevant decision makers. The current intelligence function of the EU is divided over an array of actors, who together form the European intelligence community. The European intelligence community consists of national intelligence and security services, and European information agencies. The relevant European information agencies are the European Police Organization (Europol), the Joint Situation Center (SitCen), the Intelligence Division of the European Union Military Staff (INTDIV EUMS), and the European Union Satellite Center (EUSC).
These four bodies are explicitly called information agencies instead of intelligence agencies, since they fulfill 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. Furthermore, their customers are both national intelligence services and EU decision makers. Thus, the four mentioned bodies fulfill part of the intelligence function of the EU. However, since they are not intelligence services, they will be called information agencies throughout this study.

This research concerns intelligence-led law enforcement in the EU and its counter-terrorism policy. Police and intelligence cooperation are considered under this heading throughout this study. Having said this, the difference between police cooperation and intelligence cooperation is important and should be mentioned at the beginning of the study. In terms of fighting terrorism, police forces and intelligence services do their work at different points in time. Intelligence services conduct investigations and do research preferably before a terrorist attack takes place: they attempt to prevent the attack (pre). Police forces, on the other hand, usually perform their duties after an attack takes place (post). This is one of the most important differences between police forces and intelligence services when fighting terrorism. Throughout the study, they will be treated similarly. Where important distinctions exist, these will be mentioned.

Most definitions of law enforcement exclude intelligence services. The term “law enforcement agency” is used for any agency that enforces the law, and usually refers to any type of police service. Since intelligence and security services normally do not have the power to enforce the law (since they cannot arrest individuals), they are usually left outside the definition of law enforcement. However, for the purposes of this study, law enforcement will include the national intelligence and security services. This choice was made because they, too, enforce the law: they investigate individuals and groups who do, or intend to, break the law. For national and European counter-terrorism policy, intelligence services play a crucial role. Intelligence services will thus be included under the heading of European counter-terrorism law enforcement.

The EU’s Pillar Structure

This research mostly concerns topics that are located firmly within the EU’s Third Pillar, now named Police and Judicial Cooperation and Criminal Matters. The Third Pillar houses topics such as terrorism and organized crime. International police cooperation belongs to the Third Pillar. However, it should
be mentioned that some of the researched topics also belong to the EU’s Second Pillar. The Second Pillar, named Common Foreign and Security Policy (CFSP), deals with topics such as European security policy. The interaction between the Second and Third Pillar (such as CFSP operations in the Balkans having implications for organized crime and human trafficking) is relevant for all processes of information sharing in the EU. Therefore, this research can be said to move on the fault line between the EU’s Second and Third Pillar, and it incorporates elements from both pillars.

The INTDIV and the EUSC fulfill functions mainly in the context of the Second Pillar. They are of lesser relevance to this study than SitCen and Europol, which have a specific counter-terrorism mandate under the Second and Third Pillar. The focus of this study will therefore lie with the two European information agencies that have a specific counter-terrorism mandate, Europol and SitCen. Where relevant, also the EUSC and INTDIV will be discussed, since both do play an important role in the overall EU intelligence community.

Topic delimitation

The scope of this research is restricted to the exchange of intelligence between EU Member States and designated EU information agencies to combat terrorism. Many related topics will not be the subject of this research. For instance: intelligence exchange with other states and/or organizations, intelligence cooperation outside the European Union, the use of intelligence in prosecuting (potential) terrorists, privacy and accountability, the impact of intelligence sharing on human rights or fundamental freedoms, etc.

The study intends to provide policy makers and operational personnel with more options and incentives for intelligence sharing. The intended actors to share intelligence are officers from the national security and intelligence services. Thus, operational personnel and policy makers in the field of national intelligence and security agencies are the intended recipients of this research.

The need for increased security for European citizens is often said to go hand in hand with an endangering of their fundamental freedoms and civil liberties, most notably their right to privacy. For instance, the US Patriot

---


Act, adopted after 9/11 has often been accused of doing damage to the fundamental freedoms and civil liberties of citizens worldwide and Americans in particular. This discussion is valid and crucial for the development of European intelligence cooperation. However, the balance between security and privacy is a subject of its own. The topic is too large to be included in this study.

The four mentioned EU information agencies (Europol, INTDIV, SitCen, and the EUSC) have all been the topic of research. Unfortunately, the timeframe did not allow for a visit, or for extensive research on the EUSC. Therefore, substantially less information on the EUSC is available in this research. In any case, their role in the EU’s counter-terrorism policy, compared to the other three agencies, is relatively small. Where information on the EUSC was available, usually from desktop research, literature study, or interviews, this has been used and indicated.

**Intelligence-led law enforcement**

The EU’s stated goal is to move to a policy of intelligence-led law enforcement. The EU Commission says “the police and judicial authorities are to be encouraged to enhance cooperation through intelligence-led actions. The Commission intends to make the necessary information available to a criminal intelligence network and to format this information so that it can be used throughout the EU. The aim is to improve the security of the EU and its citizens while respecting individuals’ fundamental rights and the rule of law.” Improved counter-terrorism intelligence cooperation will help the implementation of EU intelligence-led law enforcement.

The EU is currently exhibiting a growing awareness that any concerted response to terrorism requires increasing pooling of data and information at the minimum and the establishment of a true European intelligence agency at the maximum. However, no European intelligence agency exists at this time and none is envisaged for the near future. Yet, the fact that the EU formulates and implements its own security policy, means that a credible EU intelligence structure has to be put in place to support this security policy. The EU’s intelligence function needs to be reinforced.

---


1.2 Literature review

Although intelligence sharing is seen as the most promising tool in the EU’s fight against terrorism, operational personnel, policy makers and academics alike are skeptical. The topic of intelligence sharing, and especially more intelligence sharing, is seen as an area where change is unnatural, unlikely, and at best scenario: slow.

However, this does not make research in the area of intelligence sharing unpractical and idealistic. This study builds on assumptions that aim to depict a realistic picture of the intelligence community within the European Union and its current sharing practices. Building on these realistic assumptions, this research aims to develop an efficient and down-to-earth strategy to improve intelligence sharing within the European Union. The fact that something is difficult does not mean that an attempt to improve it is entirely meritless.

International intelligence cooperation

In order to present a coherent and consistent set of analyses and recommendations, it was necessary to create a frame of reference for this study. This frame of reference consists of a set of results, gained from literature study, which are assumed to be true about intelligence sharing in general, and more specifically, intelligence sharing in the European Union. The following conclusions about intelligence exchange in the European Union have been assembled from the available literature, and together form the frame of reference for this research. The frame of reference aims to depict a realistic picture of the assumptions that determine the behavior of operational personnel when sharing intelligence.

The conclusions about the European intelligence community can be divided into four categories: state sovereignty and the nature of the intelligence community, the protection of interests, what intelligence is shared and types of intelligence exchange. This list of results implies that improving intelligence sharing within the European Union will be a difficult and daunting task. However, especially in the field of stimulating informal cooperation, many improvements can be made. This research aims to discover and develop strategies to improve European intelligence cooperation, based on these assumptions.
A. The nature of the intelligence community

- Intelligence lies at the heart of state sovereignty. Intelligence is essential to state security. Intelligence sharing is counterintuitive for intelligence services.

- The intelligence community is slow to change. The new rule ‘intelligence belongs not to those who find it, but to those who need it’ is not a basic assumption for the European intelligence services. The concept of intelligence-led law enforcement is not yet engrained in the European intelligence community.

- Esprit de corps leads each intelligence organization to have absolute faith and confidence only in its own work.  

- The conservative nature of intelligence agencies coupled with the bureaucratic lethargy of the EU slows intelligence cooperation in the EU.

B. Protection of interests

- Intelligence services will only share intelligence if they receive intelligence in return. This rule is called “quid pro quo”. Sharing of intelligence must improve the information position of an intelligence service on a certain topic.

- Intelligence services fear spoiling the privileged relationship with another significant partner by sharing their intelligence with other countries.

- The recipient of intelligence sharing could take actions which could be contrary to the intelligence sender’s interest. This decreases the sender’s will to share.

- Intelligence services do not want their shared intelligence to be passed on to third parties, whose reliability is unknown. The so-called ‘third party’ rule means that any received/shared intelligence cannot be shared with any other service or country. Services do not trust third parties to keep their intelligence classified or secret.

- Intelligence services do not want to share intelligence that could give them a relative advantage over rivaling intelligence services within their own country.

---

6 Becher, K. Et al. (1998) Towards a European Intelligence Policy, Institute for Security Studies of WEU, 01-Dec-98, EU ISS paper Chaillot 34.
C. Which intelligence shared

- The likelihood to share a certain type of intelligence is inversely related to the “actionableness” of this intelligence. Put more simply, ‘hot’ intelligence is least likely to be shared. Reports comprised of Open Source Intelligence (OSINT) are most likely to be shared.

- Intelligence services are most hesitant about revealing the sources of their intelligence. They also do not want to reveal gaps in their sources or intelligence. Any shared intelligence will likely be ‘sanitized’, so it can no longer be traced where the information came from.

- Intelligence services are more likely to share analyzed reports than raw information. They fear the disclosing and compromising of their sources.

D. Types of intelligence exchange

- Intelligence personnel prefer to rely on sharing intelligence with persons they know. Intelligence is mostly shared with trusted friends and colleagues. Building these relationships of trust can take years. In intelligence sharing, people and personal relationships (‘chemistry’) matter. Even within one institution, informal channels for information sharing are extremely important.

- The international structures for intelligence sharing are poorly equipped and not transparent. Structures are too complex and bureaucratic to connect smoothly with daily operations of intelligence officers. The influence of EU instruments to stimulate intelligence cooperation on actual intelligence cooperation is limited.

- The better a formal arrangement for intelligence sharing is grounded in the professional reality of intelligence professionals, the higher will be its influence on the practice of intelligence cooperation.

- Cultural and language problems exist between intelligence services from different countries.

- Intelligence sharing is hampered by legal problems, mainly involving privacy legislation.

- There is considerable potential for non-bureaucratic, semi-operational networking and intelligence sharing within the EU that is not confined to the rules and procedures of the Brussels bureaucracy.
1.3 Methods

This research relied on different methods of information gathering, study, analysis and recommendations. Under this section, the methods of information gathering and analysis will be described.

Starting in June 2006, desktop research\(^7\) was used to gather information about counter-terrorism intelligence cooperation in the EU. Using books, academic journals, Internet portals, government reports, and research studies, the frame of reference of this research was designed from the conclusions of the literature study. The literature ranged from general books and articles about intelligence, counter-terrorism, EU counter-terrorism policy to the use of intelligence to counter terrorism. Literature analysis was also used to formulate the interview protocol. A bibliography of the used literature is attached as chapter 8 to this study.

The research aimed to combine this theoretical and academic background from the literature with the practical opinions and ideas of operational personnel and policymakers. The research maintained a strong policy emphasis. The research employed qualitative methods of research. Qualitative methods were used because the goal of the research was to explore people’s subjective experiences and meanings they attach to such experiences.\(^8\)

The interviewees were selected based on two criteria. The first criterion was extensive knowledge, academic or practical, on the topic of European intelligence sharing. Some professors and practitioners from the field were interviewed on the basis of this criterion. The second criterion was experience with European intelligence sharing. Interviewees from national intelligence services and EU information agencies were interviewed on the basis of this criterion.

The interviews were held on the basis of an interview protocol. This interview protocol was based on the findings of the literature study. It aimed to arrive at a host of answers to the original research question. The interviews were semi-structured. The protocol was used as the basis of the questions, but interviewees were stimulated as much as possible to speak about their own experiences with intelligence sharing. Thus, open-ended questions

---

7 Desktop research consists of researching books, magazines, (academic) journals, newspapers, periodicals, databases, webpages, etc.
and informal probing was used to collect as much information as possible from the interviewees. The protocol functioned as a checklist of topics to be covered, but the order of topics was not preordained. The protocol is attached as chapter 11 of this study.

During the interviews, the first part of the interview usually concerned the position of the interviewee within the organization, and the role and experiences of the organization within the larger framework of EU counter-terrorism policy. The second part of the interview usually concerned the interviewee’s personal experiences with intelligence sharing, and their opinions on formal versus informal arrangements of information sharing.

Open-ended questions were used to allow interviewees to talk at length about a topic, such as the use of personal contacts when sharing information. Various forms of probing (“can you explain that more?” “can you elaborate?”) were used to ask the interviewee to elaborate on a topic of particular interest to the research.

Most of the interviewees were visited in person, and the author of the study was personally in charge of the interviews. Some other academics, professionals and practitioners were consulted over the phone or by email. The interviews were conducted in the Spring of 2007.

Based on the interviews, extensive notes were taken. These interview reports were then analysed and compared with the findings of the literature study. The findings of the interviews constituted the data that was analysed and interpreted. Academic methods of literature analysis were used, but the study was written towards application-oriented results.

Stays at research institutes and relevant organizations were executed in the Winter and Spring of 2007. Two research stays were incorporated into the study: Europol (The Hague) and the International Institute for Strategic Studies (London). Various other institutions were visited for interviews. For a complete overview of visited institutions, research centers and think tanks, please refer to chapter 9.

1.4 Research framework

This section seeks to explain what research framework has been used throughout the study. The emphasis of this study lies on the application of recommendations, and thus on the practical framework. However, to
determine the behavior of individual intelligence officers, some academic theories can be rather loosely applied. The academic research framework will be used mostly to explain the behavior of individual intelligence officers, rather than organizations (such as a national government) or organizational components (such as a national intelligence service or an EU information agency).

**Academic Framework**

In terms of academic research, intelligence cooperation is an interdisciplinary field. It has aspects of political science, international law, public administration, European law, international relations, strategic studies, but also of police studies, economics and psychology. Therefore, it has no added value to select one single field of theory as the academic framework for this research. Rather, the research will draw on different theoretical academic fields, most importantly political science, international police cooperation and psychology.

A possible theory to explain the behavior of individual intelligence officers when sharing intelligence is rational choice theory. While recognizing that human motivation is complex, rational choice theory assumes that individuals are self-interested. It assumes that each action has a known outcome, and individuals can choose with capacity, time, and emotional detachment about the course which is most in his or her self-interest by weighing costs and benefits, risks and rewards.

In practice, intelligence cooperation can be viewed from many angles: organizational, financial, legal, technical, political, culture and attitudes (informal cooperation), symbolism, etc. This research aims to identify which of these aspects is most promising in stimulating intelligence cooperation. Of interest, especially, is the ‘culture and attitudes’ aspect in intelligence cooperation, and all informal aspects of cooperation.

International cooperation in the law enforcement field (most notably police cooperation) is often analyzed from a sociological and/or political perspective. Theory from international relations (IR) plays an important role in analyzing international police and security cooperation. The theoretical framework of psychology or economics is hardly ever used to analyze this type of cooperation, although it could explain the behavior of the persons actually exchanging the intelligence. This research aims to adopt a more psychological-economical framework to analyze international intelligence cooperation. This
perspective could also explain why states and organizations decide to share intelligence, with whom, and in what formats (i.e. where they will spend their time, personnel, and resources).

Thus, the focus of this research will be much more on actual persons (operative personnel actually sharing the intelligence and policy makers who have to make the decision to start sharing intelligence) than on states or organizations, which from the outside seem to act more like black boxes.

### 1.5 Definitions

**Information versus intelligence**

An important difference exists between information and intelligence, even if the terms are used interchangeably in many newspapers and articles. Information means raw data that has not been processed. Intelligence is selected, combined and analyzed information that aids decision makers. It consists of validated information from different sources.\(^9\)

The definition of intelligence that will be used in this research thus has two essential elements. Firstly, it is processed, analyzed and validated information that comes from various sources. Secondly, all intelligence is produced to aid decision makers. In sum, the following definition of intelligence will be used throughout this research: ‘intelligence is analyzed and validated information, preferably coming from various sources, that is produced to aid decision makers.’ This research focuses on counter-terrorism intelligence sharing: thus, intelligence that can be used to combat terrorism.

This being said, the terms ‘intelligence sharing’ and ‘information sharing’ are often used interchangeably in this policy field. The EU has initiatives on ‘information sharing’, even though the majority of this information, in reality, is intelligence. In this study, the terms information sharing and intelligence sharing will also be used interchangeably.

Sharing and Exchanging

The difference between intelligence exchange and intelligence sharing is relevant for the works of Europol, even if the two terms are often (also in this study) used interchangeably. Intelligence exchange takes place between two parties: national police forces or intelligence services, or a national police force or intelligence service and Europol. The information is received by two parties; they exchange information.

Information sharing, on the other hand, goes a step further. It assumes the presence of an ‘information clearing house’. Such an information clearing house would act as the central hub amongst many relationships of intelligence sharing within the EU. In this role, all Member States would submit all relevant intelligence to this clearing house. This actor would analyse and verify the intelligence, and distribute it amongst the relevant parties. If Europol manages to play the role of a clearing house within the European intelligence community, its main task would be intelligence sharing. Thus, information is received by Europol from a national police force. Consequently, this information can be accessed (controlled by Europol) by other Member States, if it is relevant for them. In this manner, organized crime and terrorism can really be combated at a European level, instead of merely bilaterally. Information is interpreted and then used by many parties.

Terrorism

The US Department of Defense defines terrorism as “the unlawful use of – or threatened use of – force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives.” The EU provides that terrorist offences are certain criminal offences set out in a list comprised largely of serious offences against persons and property which, “given their nature or context, may seriously damage a country or an international organization where committed with the aim of: seriously intimidating a population; or unduly compelling a Government or international organization to perform or abstain from performing any act; or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization.”

11 COUNCIL FRAMEWORK DECISION of 13 June 2002 on combating terrorism, (2002/475/JHA)
In this study, terrorism will be seen as a crime. Thus, counter-terrorism could benefit from the implementation of and adherence to intelligence-led law enforcement, which was designed to combat and prevent crime. However, it is understood that terrorism implies more than merely a violation of the law: many aspects of safety and security, public order and crisis management are involved in the combating and preventing of terrorism. Thus, counter-terrorism policy covers a broader base than mere crime prevention.

For this study it is necessary to make a distinction between so-called old and new terrorism. This difference will be elaborated upon in chapter 2.

### Intelligence-led Law Enforcement

Intelligence-led law enforcement refers to the more effective use of information to achieve better results in law enforcement. Put more simply, intelligence-led law enforcement smartly combines the strategic information with the operational to achieve better crime-fighting results. The use of information in this case goes in both directions. The law enforcement agencies provide better information to the public, in order to prevent crime. The public provides better information to the law enforcement agencies, which are then more capable to put this information to effective use. This is also called community policing.

An example of intelligence-led law enforcement and community policing is the strategy to provide the public with information about activities and signs to be aware of and to explain what to do with information related to potential threats. Furthermore, intelligence-led law enforcement relies on using information from line-level personnel, being able to adapt to new or changing threats, and constant feedback that assess successes and failures of strategic responses.\(^\text{12}\)

Intelligence-led law enforcement also implies changes for the methods and sources of the use of intelligence. For instance, the arrests following the London subway and the Madrid train bombings used intelligence from surveillance cameras, community informants and prison officials. Recent arrests of suspected terrorists in the US, Canada and the UK suggest that intelligence may be able to identify groups and allow for intervention prior to attacks.\(^\text{13}\)

---

Intelligence-led law enforcement so far has been used mainly to prevent and combat most forms of crime, excluding terrorism. Terrorism was explicitly excluded because it is sometimes not viewed as a traditional crime. This is unfortunate, given the fact that terrorists are usually involved in a wide variety of routine and preparatory crimes. An understanding of intelligence-led law enforcement that encompasses all crimes, including terrorism, increases the likelihood of identifying links between criminal activity and terrorist threats, such as drug trafficking as a funding activity. Thus, intelligence-led law enforcement works at its best when it is applied to all forms of crime, and is integrated throughout all law enforcement agencies in EU Member States. The stated goal of implementing intelligence-led law enforcement will yield good results for European law enforcement.14

Thus, intelligence-led law enforcement introduces some important terms and understandings, which are crucial for law enforcement agencies to keep up with the changes in the security environment. Law enforcement agencies need to be effective consumers of intelligence products, meaning they must be able to put received information to maximum use in the minimum amount of time. Furthermore, they need to develop a culture of collection, where personnel of all levels engage in gathering relevant information from all sources available, including many non-traditional. Intelligence-led law enforcement should be operationally integrated within the entire organization of the agency and its partners. Increased information sharing should take place with broader public safety agencies and the private security sector. Intelligence should be routinely used to make better tactical and strategic decisions. Lastly, the concept of community policing plays an important role in intelligence-led law enforcement.15

1.6 Reading guidelines

The present chapter will function as an introduction, introducing the leader to the topic of the research, the thesis and the definitions used throughout the study. Chapter 2 provides some necessary theoretical and practical background to the research on the changing security environment. Chapter 3 described the manners in which intelligence can be used to combat terrorism. Chapter 4 is a description of the EU intelligence community. It describes the

actors in this community, and the manners in which they interact and share information. Chapter 5 maps the general problems in intelligence sharing in the European intelligence community. Chapter 6 treats one of these problems, namely on informal sharing and the use of personal contacts to build a culture of trust, more elaborately. Chapter 7 contains the recommendations of this study.
Chapter 2

The Changing Security Environment of the EU

2.1 Introduction

This chapter aims to provide the necessary background to understanding the EU in a changing security environment, and especially the way it aims to fight terrorism through improved intelligence exchange. The following text is not intended to provide a complete explanation of the developments in terrorism or in the security environment of the 21st century. It is meant to provide the necessary background to understand the security environment in which the EU currently functions. This chapter will discuss the developments in terrorism, intelligence, and how the EU is behaving as a security actor under such developments.

2.2 The changing security environment

Keeping a realistic perspective on European security is essential. Europeans are safer than ever before – from diseases, from war, from accidents. Yet a declining level or risk tolerance (even small threats to security are not accepted) causes a greater level of insecurity. This “threat of securitization” needs sound and responsible political management.1

---

Chapter 2

Developments in Terrorism

Much has been written on the changing security environment of the last decade. Especially since September 11th, 2001, the security environment has changed so substantially that much of which was valid before, has limited meaning in today’s policy making. The terrorist attacks of the last five years have had a dramatic impact on security thinking and policy. Below, some of the most important changes in terrorism are described.²

Terrorism will likely remain an important threat for years to come: terrorism has a long history, and will never completely disappear. Societies will have to learn how to live with the threat of terrorism: governments should aim to control this threat as much as possible. Democratic societies create freedoms for citizens and organizations: but these freedoms can also be misused by terrorists. Therefore, the threat of terrorism will be one of the prices to be paid for living in an open, democratic society such as the European Union.

‘New’ terrorism has diffuse objectives. It is active on a global scale and increasingly transnational in scope. This ‘new’ terrorism is more loosely organized than terrorist groups of the seventies and eighties. The internationalization of terrorism causes increasing problems in fighting it. Terrorists do not respect borders; terrorist networks interact and cooperate transnationally, sometimes more easily than law enforcement agencies from different countries. Although the difference with ‘old’ terrorism is relative, new terrorism requires new ways of fighting it. The European Union will have to be prepared to fight ‘old’ and ‘new’ terrorism at the same time. Terrorists will use combinations of ‘old’ and ‘new’ tactics (such as cyber terrorism, net wars, NBC weapons) to achieve their objectives.

Terrorism and crime are ever closely interlinked. Organized crime in many forms (drugs, weapons, trafficking) has always been a popular manner to finance terrorist networks. However, recent years have seen an ever closer linking of terrorism and crime. Virtually all large terrorist networks use organized crime to finance their actions. State support for terrorist networks has largely disappeared; some networks have wealthy private donors; but most rely on crime to fund their activities. This has implications for the counter-terrorism policy of national and European law enforcement.

There does not appear to be one single, all-efficient solution for terrorism. Terrorism is too complex to be solved by a single solution. A combination of activities (legal, technical, financial, social, intelligence, etc.) will have to be employed to decrease the threat of terrorism; combating terrorism will always have to be a mix between repressive and preventative measures. Intelligence will play an increasingly important role in fighting terrorism. Good use of intelligence can prevent terrorist attacks; can facilitate repressive measures, and makes arresting (potential) terrorists easier. This will be further discussed in chapter 3.

Fighting terrorist financing is only partially effective. Politicians and law enforcement officials have high expectations of fighting terrorist financing. ‘Follow the money’ is a popular saying in the counter-terrorism world. However, the enthusiasm for these measures has been tampered because of its relatively low success rate. Fighting terrorist financing is useful, but only in combination with other repressive and preventative measures.

The media and communication with the general public is becoming more important for terrorist organizations and networks. Terrorist actions (“breaking news”) are important for media. But the extensive media attention for terrorist attacks is a way for terrorist to further broadcast their message.

New Terrorism versus Old Terrorism

A large debate exists about whether ‘new’ terrorism has decidedly different characteristics than ‘old’ terrorism. None of the so called ‘new threats’ such as terrorism, proliferation and organized crime are new phenomena as such. However, the novelty lies in the qualitative changes of these crimes, which results from a combination of several factors. Fukuyama argues that the “new threat” lies in the combination of radical Islamism and weapons of mass destruction. Both have existed for a long time as threats to EU security, but their combination is causing a new security environment.

---

‘Old’ terrorism was characterized by using terrorism as a means to further an ideological or territorial goal. Examples of organizations employing these ‘old’ terrorist tactics are the Front Libération de Quebec, IRA, ETA, PLO, RAF, Brigate Rosse, the Japanese Red Army, Tupamaros (Uruguay) and the Sendero Luminoso (Peru). Terrorist tactics used by these organizations included targeted assassinations, the taking of hostages and kidnappings.

‘Old’ terrorism is not a concept of the past – these tactics can and will be used also in the future. Several nationalist groups still employ old terrorist tactics, which currently account for the large majority of terrorist incidents in the EU.6

The threat of the ‘new’ terrorism has been added as a new element. The ‘new’ terrorism has new goals and rather nondescript goals, such as the rejection of Western lifestyle or the creation of a regime with different dominant norms and values. Most visible in this respect is Islamist terrorism, but different religious sects in Asia are pursuing similar goals.7 The current perceived threat of terrorism against the EU and its Member States is posed by Islamist and non-Islamist networks.8 The majority of terrorist attacks within the EU are committed by nationalistic groups and political extremists.

Another characteristic of the new security environment is that it does not focus only on the state level. The dividing line between genuine military, terrorist, proliferation, criminal, and sometimes even humanitarian threats is increasingly blurred.9 Terrorism has been noted to be increasingly mingled with other criminal activities, such as narcotics, weapons trade, human trafficking, money laundering and forgery, fraud, corruption, and the smuggling of nuclear

---

substances. Terrorists are becoming more skillful at using the media to achieve their objectives: the posting of decrees and films online both attracts new followers and further intimidates the general public.

Experts on Islamist terrorism, such as Roy and Kepel say that it is not rooted in cultural or religious terms, but that it represents a form of “deterritorialised Islam”, in which individual Muslims find themselves cut off from authentic local traditions. According to them, Islamist terrorists attempt to create a new, universalistic doctrine that can be a source of identity within the context of the modern, globalised, multicultural world. It ideologises religion and uses it for political purposes. The threat is mostly posed by alienated and angry youth in European cities, who seek jihadist ideology as an identity.

The objective of terrorists is often to intimidate and frighten societies. What can be witnessed is that in some ways, terrorist networks are achieving their objectives: societies are intimidated by the constant threat of terrorism and behave likewise. This signals the transformation from ‘terrorism’ to ‘terror’.

Concluding, the terrorist threat that faces the European Union is characterized by its increasingly transnational scope, the lesser degree of predictability, and the fact that individual Member States are weaker in controlling persons and groups.

The threat of Al-Qaeda and Islamist terrorism

Despite the fact that serious blows have been dealt to this organization (in the form of destruction of its infrastructure, the bombing of its training camps, the arrest of leaders and the continued hunt for its inspirator Usama bin Ladin), it continues to pose a threat to the United States and the United Kingdom in particular. Jessica Stern (author of “Terror in the Name of God: Why Religious Militants Kill”) argues that over its life span, Al-Qaeda has constantly evolved and shown a surprising willingness to adapt its mission. Ensuring the survival

of a terrorist group demands flexibility in many areas, but especially in terms of mission. Al-Qaeda started as an organization devoted to fighting Soviet forces in Afghanistan and providing logistical support to the muddjahedin fighters. Al-Qaeda’s goal was said to be the removal of Western troops from Saudi Arabia (holy land for Muslims). The importance of the Palestinian struggle and the Arab-Israeli wars, and the rejecting of Western lifestyle have grown over the years. The underlying message has become to restore the dignity of humiliated young Muslims.

The International Armed Conflict Database of the International Institute of Strategic Studies (IISS) describes Al-Qaeda as a network linked with Islamist struggles around the world. It focuses on non-Muslim nations viewed as enemies of Islam, principally Israel and the US. Their strategy entails terrorist attacks on targets symbolizing the enemy’s might. Al-Qaeda and several Jihadist groups with similar goals continue to provide threats to the security of European citizens. August 2006 witnessed a major attempted attack in the UK in which ten US-bound aircraft were targeted. The British security services were able to thwart the plot which sought to detonate liquid explosive devices smuggled on to passenger aircraft in hand-luggage.16

However, it is essential to keep a relative perspective on the threat of terrorism to the EU. As was described in the introduction of this chapter, the EU is safer than ever. The Armed Conflict Database of the IISS puts the number of fatalities related to international terrorism to an average of 530 persons each year in the period between 2002 and 2006.17 Plus, these fatalities were counted world-wide: only a small portion of them are due to terrorist attacks in the EU, such as the bombings in London and Madrid. Thus, maintaining a realistic perspective when discussing the threat to terrorism to the EU is essential.

### 2.3 Developments in intelligence

Intelligence has changed alongside terrorism. Some developments can be distinguished that today are forcing national intelligence and security services to change their modi operandus.
The Changing Security Environment of the EU

Targets

European and national intelligence agencies focus on a much wider range of potential targets, all of which are individually of lower priority targets than during the Cold War. These targets could be formed by individual cells of larger terrorist networks, individuals planning attacks, or larger, loosely organized networks of potentially violent fundamentalists. Often, these targets do not appear on the ‘radar screen’ of intelligence agencies until they use violence. Sleeper cells and individuals can usually operate outside the watch of law enforcement authorities. Hence, the new terrorists are “networked global agents [who] are blending political and religious fanaticism with criminal enterprises to challenge the rule of law and exploit the seams between crime and war.”

The geographical focus of intelligence services on closed societies has shifted to topics such as proliferation of WMD, protection of vulnerable targets and terrorism, regardless of where they may occur. Although failing states are still targets of interests for most intelligence services, the focus lies now much more on non-state entities.

Sources

European and national intelligence agencies are also experiencing the consequences of the information revolution of the last decade, caused by the increasing availability of an increasing amount of information. Not only are open sources more widely available, but the boundaries between open and covert information are also blurring. The best example of this development is the availability of satellite images of the earth free of charge through programs such as Google Earth. The proliferation of civil Earth Observation Satellites and improvement in imagery analysis techniques are rapidly eroding the monopoly on IMINT formerly reserved for the US and the Soviet Union. Sources are thus increasing, but it is increasingly difficult for intelligence services to monitor and detect activities of persons and groups.

Another important development lies in the distinction between collection and analysis. Often, national intelligence reform stipulates the augmentation of collection capabilities for national intelligence services. However, the problem with the developments in intelligence lies not in collection capabilities, but in analysis capabilities. The exploding amount of information needs to be selected and processed to form high quality intelligence products. For the EU intelligence function, better selection and analysis has priority over the acquisition of collection capabilities. More sources, more information and more intelligence are not always the solution: more often, better analysis and selection of available sources is needed more urgently than more information.

Furthermore, intelligence needs to increase its focus on sharing to achieve better results from cooperation. The possibility to share a piece of intelligence will greatly increase its value in today’s intelligence world. The change occurs from ‘need to have’ to ‘need to share’ and from ‘right to share’ to ‘write to share’.

Methods

The key to good intelligence is all source assessment, meaning an analysis of validated pieces of information from different sources. The capabilities of most intelligence agencies are focused on Cold War scenarios and have mostly not made the transition to the security challenges of today’s threats and missions. For instance, most intelligence agencies are designed to investigate state entities and armies, whilst today’s threats are mostly posed by flexible non-state actors. The new complex of issues surrounding these contingencies involves less traditional hard military net assessments and diplomatic intelligence, and more soft analysis of complex political, paramilitary, social, economic and technological issues.

New intelligence

The traditional approach towards intelligence differentiates between security and intelligence, between criminal intelligence and security intelligence, and between domestic and international intelligence. Such differences are no

The new approach to intelligence recognizes the value of all these types of intelligence in combination. Thus, new intelligence consists of open source information, COTS (commercial off the shelf) products, public databases, academic research, products from think tanks and research institute, information supplied by diplomats, military personnel, international students and frequent travelers are sources of information. These were not previously regarded as intelligence, but now constitute an invaluable source of it. The scope of intelligence needs to merge from military or civil to military-civil; from national or international to both; from state or terrorists to state-sponsored terrorism.

In making all-source assessments with added value in today’s intelligence world, soft as well as hard capabilities are needed. This means that intelligence services rely –as they did before- on covert methods of collecting information. Yet increasingly the focus also lies on softer methods such as better use of OSINT, and the collection of information through semi-covert methods, such as information collection by diplomats, soldiers, and international students.23

The nature of threats requires the gathering and analysis of information that is not constrained by territorial borders or organizational structures. Such threats have increasingly come from terrorists, fundamentalist religious movements, and less from other sovereign states.24 The methods adopted by national and European intelligence services need to rapidly adapt to this change.

A further change for intelligence services lies in the type of partner available for cooperation agreements. Whereas intelligence services used to only cooperate with intelligence services, now they are required and sometimes forced to cooperate with a variety of other institutions, ranging from universities, international organizations, think tanks and research institutes. Furthermore, intelligence services are being pressed by civil society within most EU Member States for more openness, transparency, civil consultation and participation in the political debate.25

---

Chapter 2

Intelligence agencies also need to change their human capital by focusing on people who understand public opinion and mass movements in those areas of the world where power has become much more decentralized. More economists and business school graduates are needed who understand commercial competition and fewer experts on military technology or the Soviet order of battle.26

Analysis reports of intelligence services must make better use of open sources and must be more interdisciplinary, for instance using more reports from commercial and political officers overseas.

The relationship between civilian and military intelligence is becoming more important and transcendent. Virtually no EU Member State can afford two costly and competing empires (a civil and a military intelligence service) that often find it difficult to work together in times of crisis.27

Costs

National and European information agencies are under increasing pressure to deliver ever better intelligence products at lower costs. Especially military intelligence and security agencies find their budgets are shrinking every year. Any European cooperation or even intra-agency cooperation will reduce the costs since fewer overlap will be the result of better cooperation.

Besides these four main developments, the intelligence arena is also changing in other, more subtle ways. Human intelligence (HUMINT) is becoming ever more important.28 SIGINT is a great aid to collection, but human sources are critically important to the penetration of terrorist organizations and drug rings. UK Home Secretary Charles Clarke remarked that “in many [...] cases intelligence is brought not through intercept, not through phone tapping, but by the existence of individuals within organizations we are talking about who are giving information about what is taking place.”29

27 Ibid.
28 Ibid.
2.4 The EU as a security actor

Throughout the 1990s, there has been growing political momentum for greater intelligence cooperation in the European community, as can be seen from the Maastricht Treaty, the Amsterdam Treaty, the St Petersburg tasks, and especially several international conflicts (Kosovo, Bosnia, Gulf War) which showed the European dependency on US intelligence. Two important statements which showed the EU’s intention for greater intelligence cooperation are the St. Malo declaration and the Cologne statement.30

The EU decided in 1998 at the British-French summit in St. Malo, that intelligence is fundamental to the success of the EU. It was also stated there that appropriate structures for intelligence should be instituted, along with a capacity for analysis, sources of intelligence, and relevant strategic planning without unnecessary duplication.31

Before the attacks of 11 September 2001, the EU had several strata of counter-terrorism activities already in place: institutionally, a European police bureau competent to deal with terrorism-related offences; legally, conventions and additional legal instruments to facilitate extradition; and operationally, direct and regular contact between the heads of European security services, an anti-terrorism repertory, and a regular update of the security situation.32 The impact of September 11th was that existing arrangements were invigorated, and draft agreements sailed through a political window of opportunity.

After 9/11

After the terrorist attacks of 11 September 2001 on the United States, the EU took several steps in reaction to the new security environment. Increased cooperation with the US was initiated in several areas: the identification of terrorist organizations; the participation of US representatives in meetings of the heads of EU counter terrorism unit meetings at the instigation of the EU Police Chiefs Operational Task Force (PCOTF) to share the best practices

30 Villadsen, O.R (2000) Prospects for a European Common Intelligence Policy, Georgetown University, 29-Nov-00
in counter-terrorism; four joint meetings a year of the Second pillar Counter-Terrorism Working Party and of the Third pillar Working Party on Terrorism with US representatives.\(^{33}\)

The threat of terrorism to the European Union covers a wide array of topics, networks and groups. Several international Jihadist networks operate within the EU, and the EU is a target of these networks. However, the terrorism threat to the EU also concerns other religious extremists, and violent political activists from across the political spectrum.\(^{34}\)

The most direct impact on the European intelligence community was triggered by the adoption of the Petersburg tasks by the EU in the 1997 Amsterdam Treaty, which called for intelligence analysis and sharing. Similarly, the St. Malo declaration called for sources and capacity for intelligence and intelligence analysis.\(^{35}\)

### European intelligence developments

The European Union and its Member States are responsible for the security of its citizens. This was the case before the rise of the new terrorism, but the changing security environment has emphasized this role and responsibility further. The EU security strategy notes that terrorism is a key threat to the European Union.\(^{36}\) In a mere six years, terrorism has worked itself to the top of the European agenda. At the same time it is however difficult to measure the effects of anti-terrorism efforts within the EU.

In most EU Member States, intelligence agencies are confronted with exponentially expanding expectations, yet their budgets are shrinking. National intelligence agencies are confronted with the contradictory pressure to maintain their core capabilities and to innovatively respond in new ways to different requests for information in parallel.\(^{37}\) Limited and often still further

---

33 Ibid.
diminishing intelligence budgets go hand in hand with an increasing number of hotbeds and potential and real crises which may, some day, threaten Europe’s economic and security interests.\textsuperscript{38}

Whereas intelligence sharing has always been appreciated by policy makers, it is remarkable how much politicians of late have emphasized the need for intelligence collaboration since 9/11.\textsuperscript{39} The EU’s role as a supranational organization makes it a suitable vehicle for a multilateral approach to terrorism. The European Council stated that it was determined to combat terrorism in all forms and everywhere in the world and that it would pursue its efforts to strengthen the coalition formed by the international community to fight against every aspect of terrorism.\textsuperscript{40}

Various Commission and Council proposals have been made in the area of information sharing, aiming to qualitatively and quantitatively improve the exchange of information, with regard for fundamental rights and the practicability of measures.\textsuperscript{41} The EU has agreed on the availability principle: from January 1st, 2008, any information available in one Member State should be available in all other 24 Member States.\textsuperscript{42}

The new security environment presents new challenges to the EU: it simultaneously has to respond to the needs of being a credible partner to the US in a situation of crisis, make an effective contribution to international political and military action against global terrorism, and to upgrade its own internal security measures and capabilities in the face of a dramatically increased terrorist threat.\textsuperscript{43} The EU has made small and often faltering steps towards

\textsuperscript{38} Baumel, A. (1996) Explanatory Memorandum to the Report on a European Intelligence Policy, Assembly of the Western European Union, 13-May-96
\textsuperscript{40} Communication from the Commission to the Council and the EP on measures to be taken to combat terrorism and other forms of serious crime, in particular to improve exchanges of information - proposal for a Council Decision on the exchange of information and cooperation concerning terrorist offenses, European Commission, 29-Mar-04
\textsuperscript{41} Ibid.
greater counter-terrorism cooperation. But the terrorist attacks in New York, and especially the bombings in Madrid of 11 March 2004, have had the effect of triggering a more proactive approach by the EU and dramatically enhanced information sharing efforts by the EU. It would therefore appear desirable to encourage the new approach of increased intelligence cooperation, viewing it as a way of adding to existing methods of cooperation.\textsuperscript{44} In short, increased intelligence cooperation within the EU is one of the most important European tools in the fight against terrorism.

### 2.5 Conclusion

This chapter has noted that today the EU functions in a dramatically different security environment than ten years ago. Especially the rise of ‘new’ terrorism is a credible and realistic threat for the security of the citizens of the EU. The EU has set itself the goal to fight terrorism: one of the ways it aims to do this is through improved intelligence cooperation within the European community, between individual Member States, and between Member States and European information agencies. The EU has obliged itself to provide an area of freedom, security and justice for its citizens. Better intelligence cooperation in all directions (both vertical and horizontal) will lead to more informed and realistic policy-making in the Second (Common Foreign and Security Policy) and the Third pillar of the EU (Police and Judicial Cooperation in Criminal Matters).

According to Europol’s report, the terrorist threat to the EU is posed by a wide number of groups and organizations ranging from international Jihadist networks and large scale nationalist groups to violent political extremist activists, generally involved in acts of sabotage and criminal damage.\textsuperscript{45} Counter-terrorism will remain high on the EU agenda, at least for the next generation. The problems surrounding terrorism are too complex to be quickly dissolved. Therefore, the EU should continue to build defenses against the

---


The Changing Security Environment of the EU

threat of terrorism. No radical departure from current EU policy is foreseen: it is crucial that the EU continues to focus on providing added value to the Member States, for instance through the better use of OSINT.46

Counter-terrorism policy is so close to national security and state sovereignty that Member States will lead the way for the foreseeable future. Thus, any EU counter-terrorism policy, including measures on intelligence cooperation, will be an addition and extra resource for Member States only and will not replace national policy. This being said, it does not mean that the EU has no role to play in the counter-terrorism field. If the EU succeeds in helping Member States to create an area of freedom, security and justice, this contains significant added value for the Member States. The EU has set this goal for herself, and it is expected from it by the Member States.

Intelligence itself is changing along the security environment. Intelligence agencies will find themselves needing to increasingly focus on a wider range of intelligence types. Less traditional hard military net assessments and diplomatic intelligence, and more soft analysis of complex political, paramilitary, social, economic and technological issues will be an unavoidable development.47 Intelligence agencies will have to start paying more attention to so-called community intelligence: information originating at a grassroots level in the community, which is relevant to the complete intelligence picture for a specific topic.

From the goals she has set for herself, the EU should develop a system for delivering a high-quality EU intelligence product, fused from national and some non-national contributions, to its CFSP and Third Pillar customers.48 The advantages of such an EU intelligence product would be numerous: EU decision makers would be better informed, inter alia, about threats, terrorist methods, organization of terrorist groups and thus better prepared to devise effective EU counter-terrorist policies. Member states would receive better support from European bodies. They would get assessment material from the SitCen and their police services in particular would get better support from Europol. Member states would retain the lead in the operational field

46 Interview with Officer of the Joint Situation Center. General Secretariat, Brussels, 16 April 2007.
but would be working more closely together through CTG, Europol, as well as through existing bilateral arrangements, to strengthen information exchange and cooperation.  

Thus, improved counter-terrorism intelligence cooperation and the introduction of intelligence-led law enforcement will cause better intelligence support to EU decision makers in the Second and Third Pillar. Furthermore, improved counter-terrorism intelligence cooperation will continue to provide incentives to Member States to submit intelligence to the European intelligence function, because it provides added intelligence value for them. Thus, intelligence sharing is needed because of the changes in terrorism, security and the nature of intelligence.

The use of intelligence to combat terrorism

3.1 Introduction

This chapter aims to elaborate on the concept of using intelligence, and more specifically intelligence cooperation, as an instrument of counter-terrorism policy. It will start by discussing types of intelligence, counter-terrorism measures in general, and the principles that the European Union applies when attempting to combat terrorism within its own borders. The second part of the chapter is devoted to describing intelligence as a counter-terrorism measure.

3.2 Introduction to types of intelligence

In security governance¹, there are three types of information: intelligence from open sources, strategic intelligence and operational intelligence. This research intends to focus on all three types of intelligence, since all three play a role in fighting terrorism on a European level. The next section seeks to introduce these types of intelligence and explain their relevance to this research. It must be emphasized that the distinction between operational

---
¹ Security governance is a concept that aims to provide a concrete contribution to the fight against the emerging threats posed by non-state actors; this is a flexible and interdisciplinary approach that applies the concept of governance into the security area. Through this approach, security policy-makers can identify strategic objectives and effectively allocate and coordinate resources to achieve them, using tools and dynamics typical in an international context.
and strategic intelligence is not always black-and-white. Normal intelligence reports contain both operational and strategic intelligence. Intelligence is usually defined by their method of gathering.

Open source intelligence (OSINT)

Open source intelligence is any information that can be gathered from open, i.e. non-classified sources. This includes all information that can be found in books, magazines, journals, newspapers, other publications, databases and the Internet. In general, information that can be gathered from open sources has become easier to find, due to the information revolution caused especially by the World Wide Web. For example, an article from a Korean newspaper is much easier to acquire today than ten years ago. Whereas before such an article had to be requested or acquired, for instance through the embassy, it can now easily be accessed via the Internet. Another example of the new possibilities of open source information is the satellite imagery program Google Earth. Free and openly accessible to the public, this software program allows users to view satellite images of large parts of the earth.

In all EU Member States, the mandate of national intelligence and security services is regulated by laws and decrees. Often, this legislation requires security and intelligence services to exhaust open sources before they can retrieve information from closed sources. In practice, this means that intelligence services need to do an exhaustive monitoring of open sources about a certain topic before they can—for example—intercept telephone conversations or employ agents (HUMINT). This means that open sources are almost always the starting point for intelligence services.

Open source intelligence has many advantages: it is fast and cheap. The technological revolution makes it increasingly easy to gather open source intelligence. Increasingly, open source intelligence is used to set the framework to answer a certain question: other methods of gathering information are consecutively used to fill in the blanks of this general framework. It is important to realize that intelligence services are not defined by secrecy and espionage, but that the monitoring of open sources is an essential part of their work.

Another type of open source intelligence that is important but under-used is the knowledge and information present with embassy personnel, academics, students, diplomats, businesses, universities, think tanks, and international organizations. Although these persons and institutions hold a large amount of information, these sources of information are not used very often by national security and intelligence services.
In general, it can be said that an increasing amount of information is available through open sources. Many experts argue that most of a state’s intelligence requirements can be satisfied by a comprehensive monitoring of open sources, even up to 95%. There will always be a need for intelligence from closed or classified sources but open sources will play an increasingly central role in the future of intelligence.

### Strategic Intelligence

For this research, strategic intelligence will refer to non-personal information about threats and risks. When applied to terrorism, strategic intelligence concerns - for instance - knowledge about terrorist networks and groups, how they are organized, where they are located, and what their modi operandi are. Strategic intelligence, as opposed to operational or “hot” intelligence, is not concerned with immediate threats, but provides outlooks for the future, tries to give early warnings about possible future threats, and tries to identify trends in the field. Therefore, strategic intelligence can have an essential ‘Indicator and Warning’ function. Other examples of strategic intelligence include: background and ideology of terrorist networks; financial arrangements and funding and the role of so-called charitable institutions in their funding. Strategic intelligence can also focus on states that are accused of harboring or protecting terrorist networks, such as Saudi Arabia, Sudan, and Syria. The intelligence about these states focuses on political regimes, infrastructure, military, and the type of support provided to terrorist networks.

Strategic intelligence is usually presented in the form of reports which concern periods of time of months or years. It is not direct, actionable intelligence, but aims to provide insight into motives, structures, and trends. In terms of intelligence sharing, most national security and intelligence service are more likely to share open source or strategic intelligence than

---


3 ‘Indicator and Warning’ function means the capacity to predict threats in the future. It is seen as one of the crucial functions of intelligence services. The Dutch cabinet named the ‘Indicator and Warning’ function of intelligence services “one of its most crucial tasks”. Tweede Kamer 2004-2005, 29876, nr. 3, p. 2. Accessible via http://parlando.sdu.nl.

operational intelligence. Put differently, the likelihood to share a certain type of intelligence is inversely related to the “actionableness” of this intelligence. More simply put: “hot” actionable intelligence is least likely to be shared whilst open source intelligence is most likely to be shared.

Operational Intelligence

As stated before, operational intelligence can be defined as actionable intelligence. Operational intelligence concerns personal data such as names, dates of birth, addresses, habits, and whereabouts of potential terrorists. Operational intelligence provides information about imminent or direct threats of terrorism. Since operational intelligence per definition concerns personal information, an inherent clash with privacy legislation exists. However, as was mentioned in the introduction of this chapter, the clash between privacy legislation and intelligence sharing will not be a focus of this research.5

Although the distinction between strategic and operational intelligence is important, it is not always easily made. Most operational intelligence does not exist without at least some degree of strategic intelligence. And vice versa, strategic intelligence is more valuable when it is supported by some degree of operational intelligence. The two terms are thus not mutually exclusive: strategic intelligence can contain operational information, and operational intelligence almost always includes some form of strategic information.

3.3 Measures to combat terrorism

Terrorism is a complex threat, as was discussed in chapter 2. Consequently, there is not one single, all-efficient solution to the threat of terrorism. Effective counter-terrorism strategies use tailored combinations of measures, with close coordination amongst intelligence, civilian and military agencies.6 However, there are a few underlying principles that guide counter-terrorism measures for democratic states. These principles have been designed by Wilkinson, and are quoted from the Terrorism and Political Violence. A Sourcebook.7 The EU, although not explicitly, uses these principles in its counter terrorism strategy and policy.

---

5 However, as was mentioned in the introduction of this chapter, the clash between privacy legislation and intelligence sharing will not be a focus of this research.
No surrender to the terrorists, and an absolute determination to defeat terrorism within the framework of the rule of law and the democratic process

No deals and no major concessions, even in the face of the most severe intimidation and blackmail

An intensified effort to bring terrorists to justice by prosecution and conviction before courts of law

Tough measures to penalize the state sponsor who give terrorist movements safe haven, explosives, cash and/or moral and diplomatic support

A determination never to allow terrorist intimidation to block or derail international diplomatic efforts to resolve major conflict in strife-torn regions.

The literature on fighting terrorism or counter-terrorism attempts to translate scientific findings into ‘to-do-lists’ and operational guidelines. Most counter-terrorism literature divides counter-terrorism measures into categories. A broad distinction can be drawn between preventative measures (such as anti-radicalization programs) and repressive measures (such as arresting suspected terrorists). Counter-terrorism measures can also be ordered in time: pro-action and prevention, planning, disruption, and reaction.

- Pro-active and preventative measures include preventing terrorism by fighting its causes
- Planning includes all measures that prepare a state for a terrorist attack
- Disruption includes measures whereby law enforcement, intelligence services and the police take action (such as notifying suspected terrorists of knowledge of their plans or arresting suspected terrorists) to prevent or disrupt an imminent terrorist attack.
- Reaction includes all measures that follow a terrorist attack, such as investigations, arrests, legal proceedings etc.

Subcategories of counter-terrorism measures include:

- Strategic measures, such as enlarged mandates for police and law enforcement, better coordination amongst counter-terrorism organizations, improving preparation and crisis management structures and realizing the symbolic effects of some counter-terrorism measures.
Social-preventative measures, attempting to prevent individuals and/or groups to turn to terrorism as a means to achieve their objectives. Social-preventative measures focus on the causes of terrorism, although a single analysis of terrorism causes cannot be made. A large disadvantage of social-preventative measures is its long-term timeframe.

Technical or physical measures include all types of measures that include a complex threat assessment of an object, person or process, and a tailored protection based on this threat assessment. Examples include the increased security at airports, checkpoints, access systems for buildings, etc. Many of these measures can be found in the area of guarding and securing (of people, of objects, of processes). The disadvantage of physical measures is that they offer an artificial security, because no physical measure can offer complete protection from any terrorist attack.

Financial measures include measures to stop terrorist funding, thereby severely damaging the potential for terrorists to commit attack and their underlying networks. Measures include the freezing of bank accounts and investigations into the role of so-called “charitable organizations”. So far, the results of financial measures seem rather limited.

Legal measures include enlarging the mandates of police, law enforcement, defense and other counter-terrorism organizations. These measures are almost always accompanied by a warning for the destruction of democratic states and fundamental freedoms of European citizens. Examples are: increased permission to collect information by intelligence and security services, permission to use violence, arrests can be made sooner and with fewer restrictions, punishments for terrorism are aggravated, and the rights of terrorism suspects are reduced.

Media measures are a separate category. Media and terrorism hold each other in a strange balance: the media needs terrorism, and terrorism needs the media. An important part of the citizen’s trust in a government’s counter-terrorism policy will be construed by media exposure of this policy. Government and media need to make agreements about the use of confidential information in the public sphere. Certain information cannot be made public in light of the importance of counter-terrorism policy. However, increased competition in the media causes problems in making (and keeping) agreements between media outlets and the government.

Intelligence measures will be more elaborately discussed below.

3.4 The use of intelligence to combat terrorism

Effective decision-making in counter-terrorism lies in having access to the right information at the right time. A simple increase of information flow is not the goal of counter-terrorism policy: the fundamental goal is to use that information to improve the actions that are being taken.

Most EU countries are well aware that “coordinating intelligence is at the heart of countering terrorism”. Former EU Counter-terrorism coordinator Gijs de Vries calls the collection, analysis and dissemination of timely and accurate information “essential to prevent acts of terrorism and to bring terrorist suspects to justice.” Intelligence is so central to counter-terrorism policy because good and timely intelligence gives governments the capacity to prevent terrorist attacks from taking place.

13 Block, L.(2005), European Counter-Terrorism Culture and Methodology, TerrorismMonitor, Volume 3, issue 8, 21-Apr-05.
If state governments are able to collect sufficient adequate information and intelligence about imminent terrorist attacks, they can prevent such attacks.\textsuperscript{15} Intelligence is justifiably emphasized in counter-terrorism literature. Intelligence is collected by security services, police, the military and increasingly, by civilians. Another important trend described in counter-terrorism literature is that after a terrorist attack, it is revealed that certain pieces of intelligence or warning were present before the attack took place. However, insufficient attention was paid to such warnings. “With regards to 9/11, US intelligence agencies had received some relevant information pre 9/11 but either failed to appreciate its significant or failed to share it.”\textsuperscript{16} This begs an essential question for intelligence and security services: who selects the relevant information from an unrelenting stream? Information needs to be permanently monitored; adequately educated personnel are necessary to decide on a relevant selection.\textsuperscript{17}

Not only national intelligence and security services collect intelligence as a counter-terrorism effort. Many organizations, both governmental and non-governmental, collect information on a daily basis that could be used in counter-terrorism policy. These non-intelligence services will play an increasingly important role in counter-terrorism intelligence. For instance, immigration and naturalization services are increasingly involved in counter-terrorism policy. At the stage of repression and prevention of radicalisation, significant information is collected from school officers and social workers. Intelligence services should increasingly seek to form partnerships with such institutions and organizations as they are crucial in developing counter-terrorism policy in the new security environment.

Intelligence (all open source and confidential information that can be used to prevent terrorist attacks) is crucial in minimalizing the threat of international terrorism. Counter-terrorism intelligence has three functions:

- To pre-empt and disrupt terrorist activity
- To conduct post-incident investigations
- To contribute to preventive/protective security measures.


The European Union Counter-Terrorism Strategy

The EU counter-terrorism strategy has four pillars.

- **To prevent** people turning to terrorism by tackling the factors or root causes which can lead to radicalisation and recruitment, in Europe and internationally. For instance, intelligence sharing between national intelligence services and other organizations, such as schools, building cooperation, social workers and youth employers can be used to pick up early warning signals for radicalisation. Various European cities are experimenting with such approaches, such as Berlin and Amsterdam.

- **To protect** citizens and infrastructure and reduce our vulnerability to attack, including through improved security of borders, transport and critical infrastructure. For instance, intelligence sharing between national intelligence services should take place to designate which infrastructure is critical, such as harbors and energy facilities. Intelligence services should exchange information about security procedures at European borders.

- **To pursue** and investigate terrorists across our borders and globally; to impede planning, travel, and communications; to disrupt support networks; to cut off funding and access to attack materials, and bring terrorists to justice. For instance, intelligence services and police forces should work together to locate the whereabouts of potential terrorists. Intelligence services can point other law enforcement agencies to the existence of terrorist networks.

- **To prepare** ourselves, in the spirit of solidarity, to manage and minimise the consequences of a terrorist attack, by improving capabilities to deal with; the aftermath; the co-ordination of the response; and the needs of victims. For instance, intelligence services should treat terrorist attacks as learning opportunities, in order to continuously improve their ability to detect threats. Moreover, intelligence services can aid police forces in managing the coordination of the response.

Counter-terrorism intelligence within the EU

The EU in recent years has made great advancements in the policy area of European Foreign and Security Policy and the European Defense Policy. The creation of the new European Defense Agency EDA is but one of the indications...
that the EU is taking its military branch more and more seriously. Since the EU Member States are also addressing the issue of a future European Army (beyond the current Rapid Reaction Force), it is crucial that a more coherent intelligence policy is created, even if such an army will function as a peacekeeping facility. The success of military missions relies on being well informed.19

Yet understandably, national ministers of justice and interior affairs are reluctant to hand over major responsibilities in the counter-terrorism and intelligence field to the EU. Bilateral arrangements between national intelligence services have so far yielded much better results in the fight against terrorism than multilateral cooperation on a European scale.20 However, in order to be successful in the future in the fight against terrorism, more multilateral cooperation is crucial. Terrorism is an international problem. In order to fight the threat it represents to European values, a comprehensive intelligence policy is needed on a European level.21

In short, there are many reasons why the EU should be working on a more coherent, more realistic and more high-quality intelligence policy. Reduced duplication and closer cooperation amongst Member States offers an opportunity for better and more efficient intelligence cooperation.22 Ideally, the EU should be able to offer an all-source intelligence product, composed of OSINT, SIGINT, HUMINT, TECHINT, ELINT, IMINT, etc.

**Criminal intelligence vs. security intelligence**

Intelligence is used to combat almost any type of crime. Police and law enforcement agencies use intelligence as an important tool in their fight against violence, trafficking and organized crime. Intelligence is a weapon to prevent a certain crime from taking place. As was emphasized before in this report, human intelligence is greatly valued by security services and law enforcement agencies. However, the use of undercover officers and informants remains limited. The costs and risks associated with such operations are substantial, and growing. Many of terrorist networks are closed societies and are difficult to infiltrate. Therefore, much of the intelligence gathered on

---

19 Ibid.
20 Ibid.
21 Ibid.
22 Ibid.
The use of intelligence to combat terrorism

terrorist networks and groups comes from traditional sources such as police reports, search warrants, anonymous tips, the public domain, and records management systems.²³

An essential difference exists between intelligence about criminals and intelligence about terrorists. ‘Ordinary’ criminals, and even members of groups of organized crime, often have lengthy arrest histories and numerous encounters with law enforcement officials documented on their criminal records. Terrorism is different from street-level crime on many fronts. Most crimes are the result of greed, anger, jealousy, or the desire for domination, respect or position in a group. Terrorism, on the other hand, can be committed out of a desire to ‘change’ the state of the world or of a particular nation.²⁴

Terrorists go to great extremes to avoid detection. Therefore, gathering information on potential terrorists requires intelligence services to think outside the box and to identify nontraditional sources of information. These could include the tracking of purchases, Internet, court records, handouts, radio and self-published books. Actionable counter-terrorism intelligence has the inherent problem of missing a ‘starting point’. For any kind of pre-emptive or prevention action there must exist at least one of the following: some form of target or time-specific threat, a persons or persons whose activity has ‘suspicious’ characteristics (perhaps purchases of IED-related components) or communications intercepted data.

The role of intelligence in convicting terrorists in courts of law is a controversial role. Evidence on terrorist activities that is essential for successful prosecution is frequently encapsulated in the intelligence provided by the intelligence agencies; but the admissibility of such information is questionable under the fair-trial principle of the European Convention on Human Rights.²⁵ Yet in the UK, primacy is given to the use of intelligence for the protection of the public by disrupting the activities of terrorists even if this reduces the evidence gathering opportunities for court purposes.²⁶

Understanding that national institutional harmony is the first step in effectively using intelligence to combat terrorism, some EU Member States have set up multidisciplinary counter-terrorism taskforces. These taskforces often include police, (military) intelligence, immigration and customs offices. Examples are the Contra-Terrorisme Infobox in the Netherlands, the Gemeinsames Terrorismusabwehrzentrum GTAZ in Germany and the l’Unité de Coordination de la Lutte Anti-Terroriste in France.27

3.5 Conclusion

This chapter has described various instruments of counter-terrorism policy, with a specific focus on intelligence measures. Strategic and operational intelligence, combined with information from open sources, can help to prevent, preempt, protect or prepare for terrorist attacks. Efficient and realistic counter terrorism policy is made up of strategic, social-preventive, technical, financial, legal, media and intelligence measures.

It has been emphasized that intelligence measures lay at the heart of any realistic counter-terrorism policy, but that no counter-terrorism policy can completely prevent a terrorist attack. Using intelligence to fight terrorism is different from using intelligence to fight crime: the absence of a ‘starting point’ is the most eye-catching difference.

The EU needs credible counter terrorism intelligence support, which is currently not sufficient. The EU intelligence function, in this case composed of national intelligence and security services plus the relevant EU information agencies, need to provide intelligence support to EU decision makers in the counter terrorism policy field. Also, EU information agencies need to supply added intelligence value to national intelligence services. This would mean a substantial step forward in counter terrorism intelligence cooperation in the EU.

27 Block, L. (2005), European CounterTerrorism Culture and Methodology, TerrorismMonitor, Volume 3, issue 8, 21-Apr-05.
Chapter 4

The European intelligence community

4.1 Introduction

This chapter will discuss ongoing efforts at the European level to improve EU counter-terrorism intelligence support to EU decision makers in the Second and Third Pillar. It will discuss the principle of availability and its implications for information sharing within the EU. Furthermore, it will describe four European information agencies and their role within the European intelligence community.

Within this chapter, a distinction will be made between

- Intelligence sharing between national law enforcement agencies, either bilaterally or multilaterally: national - national
- Intelligence sharing between a national law enforcement agency and a European information agency: national - European
- Intelligence Sharing between European information agencies: European - European

As has been mentioned in the introduction, three of the four mentioned information agencies have been visited by the author (Europol, SitCen and INTDIV). Less information was available on the EUSC, which moreover plays a less significant role in EU counter-terrorism policy. The two most significant EU counter-terrorism information agencies (Europol and SitCen) have been the focus of this chapter.
4.2 Description of the EU Intelligence Community

The European Intelligence community consists of all the actors who play a role in the EU intelligence function and counter-terrorism law enforcement. The community encompasses national and European actors. National actors include national intelligence services, national security services, and police organizations. European actors include the European information agencies (INTDIV EUMS, SitCen, Europol, and EUSC) but also the Council, the Commission, various bi- and multilateral working groups on counter-terrorism, Eurojust, the World Customs Organization, Interpol, CEPOL, the Task Force Chiefs of Police and Frontex.¹

Within the EU, there are four bodies that can be qualified as European information agencies. The term “European intelligence agency” is explicitly not used for these bodies. Rather, this study refers to these organizations as European “information”² agencies. These are the European Police Organization (Europol), the Joint Situation Center (SitCen), the European Union Satellite Center (EUSC) and the Intelligence Division of the European Union Military Staff (INTDIV). These bodies provide intelligence reports to decision-making bodies of the European Union, such as the Council and the Secretary-General/High Representative.

Concerning the task of fighting terrorism, Europol and SitCen especially play an important role. Europol has a coordinating task in information sharing within the European Union. SitCen monitors the security situation both in- and outside the borders of the EU. Since the large terrorist attacks in New York, Washington, Madrid and London, both agencies have seen their mandate enlarged. For instance, the Justice and Home Affairs (JHA) Council of 20 September 2001, and the Extraordinary Council of 21 September, undertook to launch some institutional innovations, such as the installation of a counter-terrorist unit within Europol. The unit is compromises of one police and one intelligence official, and was established for a renewable period of six


² As was explained before, the term information is used here instead of intelligence. This is done because these agencies are not intelligence agencies in the traditional sense of the word. However, they provide the intelligence support for EU decision makers, and handle European information sharing. Therefore, they are called European information agencies.
months. The team is requested to collaborate directly with their American counterparts. The remit of the team is to collect all relevant information and intelligence concerning the current threat in a timely manner, to analyze the collected information and undertake the necessary operational and strategic analysis; and to draft a threat assessment document based on the information received.3

This chapter discusses the tasks, interaction and roles of the four European information agencies aforementioned. All of the mentioned EU agencies retrieve their information from national intelligence and security services. They can be described as ‘desk services’: most of them have very few or no means to collect ‘raw’ intelligence: nor do they have the power or resources to confront identified threatening actors, such as investigation and prosecution.4 The EUSC is the only European information agency with collection capabilities. However, it is fair to say that these EU information agencies almost exclusively produce their intelligence reports with intelligence from national intelligence and security services.

**EU Counter-Terrorism Policy**

As has been argued, the EU has an important role to play in the fight against terrorism both inside and outside the borders of the EU. However, the most important actors in the fight against terrorism (police, law enforcement, judicial authorities, and intelligence and security services) all remain firmly under the national control of the Member States. Therefore, there is a set limit to what the EU can do to counter terrorism. The role of the EU in fighting terrorism, “is to assist Member States, not to supplant them.”5

The following statement characterizes the EU’s counter-terrorism policy and intentions.

---


There is a paradox in the EU’s role in counter-terrorism. On the one hand, the governments agree in principle that cooperation at the EU level is good […], but on the other, they are slow to give the Union the powers […] and resources […] to be truly effective. This is because national security policy […] goes to the core of national sovereignty, and governments are reluctant to give the EU powers that could interfere with their […] national security practices. The EU is working hard to coordinate national anti-terrorism policies, but it is only just starting to pursue its own counter-terrorism policies.  

Information sharing and counter-terrorism intelligence cooperation have always formed the heart of EU counter-terrorism policy. The EU has taken various decisions on the exchange of information on specific subjects. For instance, a decision adopted in 1997 requires the exchange of information between law enforcement agencies when potentially dangerous groups are traveling from one Member State to another. Various agreements have been signed with partners outside the EU on information sharing. On 20 December 2002, Europol and the US signed an agreement on the exchange of personal data. This allows the US to benefit from the operational and strategic analyses carried out by Europol on the basis of data from all EU Member States. There are numerous other initiatives and treaties at the European level that aim to improve the European flow of security information.

Concerning the exchange of information between law enforcement authorities of the Member States, the Commission has proposed an EU intelligence policy aimed at better exchange of information and intelligence-led law enforcement. In its Communication towards the Council and the European Parliament, the Commission mentions two obstacles to the free circulation of information and a move towards intelligence-led law enforcement: the compartmentalization of information and the lack of a clear policy on channels of information. In order to solve these hindrances to more information sharing, the Commission proposes three different objectives:

- To take stock and to analyze the conditions needed to improve access to, and the use and exchange of, relevant information on law enforcement
- To introduce an EU intelligence-led police and judicial policy

---

To maintain a strict balance between effective respect for citizen’s rights and an increase in state powers of obtaining and using law enforcement information.8

In short, it can be said that the European Commission is aiming for the production and use of EU counter terrorism intelligence that is high-quality in both strategic and operational terms. The development of intelligence-led law enforcement of the European Union is a key assumption for this chapter.9

4.3 The availability principle

The principle of availability is one of the main points presented in the 2004 Hague Program as regards law enforcement cooperation and emphasizes that information and intelligence should be made available.10 The principle of availability is defined to mean that a law enforcement officer in one Member State who needs information in order to perform his or her duties can obtain this from another Member State, and that the law enforcement agency in the other Member State which holds this information should make it available for the states purpose, taking into account the requirements of ongoing investigations in that State.11 EU Counter-terrorism Coordinator Gijs de Vries argued for this principle when he stated that “the mere fact that information crosses borders should no longer be relevant.”12

The availability principle is based on four documents:

- The Hague Program for strengthening Freedom, Security and Justice in the EU (5 November 2004)

---

9 Ibid.
10 Hague Programme (Council Conclusions) of 5 November 2004 (16054/04, 13 December 2004).

Proposal for a Council Framework Decision on the exchange of information under the principle of availability (12 October 2005)

Prüm Treaty (27 May 2005)

The principle of availability aims to tackle serious crime within the EU (including terrorism, but explicitly not only focused on terrorism) by more and improved information exchange within and between Member States, and with third states. It aims to facilitate police and judicial cooperation in the EU. Usually, such cooperation between Member States involves a formal request, and sometimes judicial authorization to gather or to exchange data, which can take time. The availability principle will ensure access to all data held by police, immigration and customs agencies and security agencies. Eventually, it is designed to also include non Member States, such as the United States.

Under the availability principle, information should be exchanged with as little effort as possible by minimizing formalities, permissions, and procedures. The principle of availability also concerns direct access to databases. It concerns many types of information, both from law enforcement databases as from national administrative systems, such as identity documents, driving licenses, vehicle registration, firearms licenses, and aviation and maritime registers. Under the availability principle, the following types of information will most likely be exchanged: DNA, fingerprints, ballistics, vehicle registrations, civil registers, telephone numbers and communication data.\(^\text{13}\)

The availability principle is controversial because of its possible interference with data protection and privacy laws. The European Data Protection Supervisor (EDPS) says that “the principle of availability can be justified; abolishment of internal borders calls for exchange of police information between the Member States. But one should keep in mind that this network will share sensitive data, and that sensitive data always require specific safeguards. We must not underestimate the risks of misuse, so let us introduce this gradually and cautiously.”\(^\text{14}\)


\(^\text{14}\) Ibid.
Implementation

The European Commission is of the opinion that whilst it is essential that the availability principle is complemented by appropriate data protection rules in the field of justice and police cooperation, it represents a significant step forward towards improved information sharing to fight terrorism within the EU.\(^\text{15}\) In a communication to the European Parliament and the Council, the Commission states that “it is not to permit that cumbersome proceedings of interchange of information avoid law and order enforcement and the investigation of trans-border crime in a free movement area.”\(^\text{16}\) Furthermore, the Commission has proposed key conditions to be fulfilled when the principle of availability is to be applied:

- The sources of information and the confidentiality of the data must be protected
- The integrity of the data to be exchanged must be guaranteed
- The respect for data protection must be supervised
- There needs to be appropriate control prior to and after the exchange.\(^\text{17}\)

The results of the availability principle heavily depend on how it will be implemented. The crucial question is whether the complete implementation of the availability principle will actually lead to full and direct access to law enforcement databases in other Member States, as this will definitely represent a significant step forward in European intelligence cooperation.

\(^{15}\) Press Release. The Availability Principle: EDPS wants the exchange of police information to be introduced more cautiously. 1 March 2006.


\(^{17}\) The Availability Principle (PowerPoint presentation). Prof. Julio Perez Gil, University of Burgos, Spain.
4.4 EU institutional framework for counter-terrorism

Counter-terrorism policy in the EU is divided over the Second and the Third Pillar, with the majority of policy located in the Third Pillar. This section examines more closely the EU institutional framework for counter-terrorism, put in place to provide an area of freedom, security and justice by preventing and combating crime and terrorism.¹⁸

**European Council**

The European Council plays a central role in the EU’s counter-terrorism policy. When it concerns matters of terrorism, the Council is comprised of Ministers of Justice and/or Interior and/or Prime Ministers and/or Presidents of Member States. The task of the European information agencies discussed in this chapter is to provide intelligence support to European decision makers. These European decision makers in need of intelligence support are mostly situated within the European Council: e.g. Ministers of Justice of Member States. Thus, the work of the European information agencies such as SitCen and Europol is designed (amongst other tasks) to improve the information position of the European Council.

The counter-terrorism work done by the Council is divided over two working groups. The first, COREPER II is composed of ambassadors and deals with counter-terrorism in the Second Pillar, the Third Pillar, and Financial Policy. The second, COREPER I is made up of ambassador’s deputies and deals with transport, communication, environment, research etc. The Council also hosts the Contact Group of Persons from the Member States’ Brussels Permanent Representations Dealing with All Aspects of Terrorism. This contact group acts as a central contact point for all counter-terrorism related information in the Member States’ Brussels Permanent Representations, but is not a Council working group.

**EU working groups on terrorism**

In the Third Pillar, the Council hosts three working groups in the policy field of counter-terrorism. The first, the Article 36 Committee (CATS) was set up under Article 36 of the Treaty on the EU to fulfill a coordinating role in criminal

¹⁸ Treaty of the European Union, article 29.
The European intelligence community

matters of police and judicial cooperation. It consists of senior officials from the Member States’ Ministries of the Interior and/or Justice. The second, the Terrorism Working Group (TWG) is composed of representatives of the Member States' Ministries of the Interior and/or law enforcement agencies, and sometimes national security services. It deals with internal threat assessments, practical cooperation and coordination amongst EU bodies.

The third is the Working Party on Terrorism (International Aspects). This is composed of representatives of Member States Ministries’ of Foreign Affairs, Interior and sometimes from national intelligence services and deals with issues related to external matters, threat assessments, and policy recommendations with regards to third countries and regions.19

In the Second pillar, the COTER working group is attended by the Ministers of Foreign Affairs of the Member States. It has a certain overlap with the working group from the Second EU pillar. This working group discusses topics such as UN strategies, humanitarian aid to non-EU Member States, technical assistance, best practices, and an inventory of ongoing counter-terrorism policies.

Permanent national representatives

National intelligence and security services are generally quite interested in contacts with the European Council and the Commission. They usually second an officer to the Member States permanent representation in Brussels. This serves two purposes: informing the Council and Commission officials about the activities of national intelligence and security services, and remaining updated about upcoming initiatives in areas of interest, such as information sharing.

Such seconded officers from national intelligence and security services can also be found at permanent representations at the United Nations Headquarters in New York. All formal requests to national intelligence and security services run through these national permanent representatives; they therefore are important points of contact.20

---


20 Interview with AIVD officer, 23 February 2007, AIVD headquarters, Leidschendam-Voorburg, the Netherlands.
Chapter 4

Communication systems

For information flows between the Council’s General Secretariat, the Commission and the Member States, two secure communication systems exist. Firstly, the COREU (CORespondance EUropéenne) links the foreign ministries of the Member States and the EU institutions, and is mainly used as a Second Pillar instrument (the formulation and discussion of the Common Foreign and Security Policy). The second system, called CORTESY (the COREU Terminal Equipment SYstem) handles the secure exchange of encrypted traffic between the Foreign Ministries, the Permanent Representatives, the Commission and the Council Secretariat, on matters related to CFSP. The network is now called ESDP-NET, and functions to provide a high-security link between EU staff HQ and Operational HQ in the event of an engagement of forces.\(^{21}\)

Thus, the Council receives intelligence support in its counter-terrorism task from European information agencies such as SitCen and Europol. SitCen is mostly responsible for the threat assessments and strategic information; Europol’s mandate lies with the fighting of organized crime. On the topic of counter-terrorism, the mandates of these two organizations overlap somewhat. It has occurred that reports to the Council on counter-terrorism are supplied through two different sources: Europol and SitCen. It remains a matter of discussion whether it would be better for the Council to receive one source of intelligence support, for instance through a combined product of Europol and SitCen. However, some also argue that it can be beneficial to receive intelligence support from two different viewpoints. \(^{22}\)

Counter-terrorism Coordinator

The Office of the Counter-Terrorism Coordinator is located within the Council Secretariat, and the position was filled by Gijs de Vries until May of 2007. The Coordinator’s task is to coordinate the work of the Council in combating terrorism with due regard to the responsibilities of the Commission, and to maintain an overview of all instruments at the Union’s disposal with a view to regular reporting to the Council and effective follow-up of Council’s decisions. No explicit powers have been assigned to the office, and no budget; therefore, it is unrealistic to expect substantial coordination performance from the

---


\(^{22}\) Interview with Europol Officer 2. 27 February 2007, Europol Headquarters, The Hague.
The European intelligence community

Coordinator\textsuperscript{23}. Furthermore, the power to ‘coordinate’ remains limited since the responsibility for counter-terrorism policy lies mainly with national governments, and not with the EU.\textsuperscript{24}

The future of the counter-terrorism Coordinator is unclear at the moment of writing.\textsuperscript{25} Gijs de Vries has left Brussels in May 2007, and no new Coordinator has been appointed. The decision has to be made by the High Representative Solana. The terms of reference, if a new Coordinator will be appointed, are likely to be changed.\textsuperscript{26}

Counter Terrorism Group (CTG)

An important forum for bilateral cooperation on the level of national intelligence services is the Counter Terrorism Group (CTG). Officially, it exists outside of the EU structure. This group consists of the heads of all national intelligence and security services of the EU Member States. Intelligence services from Norway and Switzerland participate as well. Under the main level group, consisting of the directors, function several subgroups, working on specific themes. The objective of the CTG is to improve international cooperation, and includes common threat assessments and discussions of initiatives to optimize operational cooperation. It is a useful operational level forum for multilateral cooperation.\textsuperscript{27}

National intelligence services see the added value of the cooperation within CTG for their own organization. CTG reports are classified as SECRET, and have more informational depth than, for instance, products originating from SitCen. The CTG works as follows: one Member States initiates a question, and has a leading role for this topic. Information is gathered from various Member States. The leading Member States then proceeds to analyze, report, and distribute this information. The CTG is also seen as an excellent forum for picking up European trends in counter-terrorism policy. Furthermore, since all partners within the CTG work on a strict need-to-know basis, the

\textsuperscript{23} Interview with IISS Officer 2, 10 May 2007, International Institute for Strategic Studies Headquarters, London, UK.


\textsuperscript{25} April 2007.

\textsuperscript{26} Interview with Officer of the Joint Situation Center. General Secretariat, Brussels, 16 April 2007.

confidentiality is virtually guaranteed.\textsuperscript{28} This leads to a greater willingness to share intelligence within this forum. In short, the factors that make CTG a successful forum are the informational depth of the products, the relevance of the products for the interests of Member States, and the confidentiality and restricted access to information.

4.5 National – national sharing

The vast majority of information sharing within the European Union consists of bilateral or multilateral contacts between Member States. In fact, national – national contacts between intelligence officers make up more of the European information flow than is popularly believed or understood.\textsuperscript{29} This is the case for information about terrorism, but also for all other fields of information within the policy field of police and law enforcement. The other two types of sharing (national – European and European – European) make up for a minority of the net amount of information sharing within the European Union.

Rules of intelligence sharing

In every intelligence exchange, the two basic principles of intelligence play a crucial role. The first principle is the “third-party principle”. This rule dictates that information that is received from a partner (usually another national intelligence service) can never be shared with a third party, without the explicit permission of the source of this information. The second principle is the “quid pro quo” principle: this rule ensures that there is a certain balance between the parties in the information exchange. Exchange needs to go both ways. However, this rule does not only concern the amounts of information exchanged (quantity), but also the value of the contents (quality).\textsuperscript{30}

Most interviewees also stress the importance of “playing by the rules”. The aforementioned rules of third-party principle and quid-pro-quo are strictly adhered to. No defection from these rules is allowed, and there is little room

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{28} Interview with AIVD officer, 23 February 2007, AIVD headquarters, Leidschendam-Voorburg, the Netherlands.
\item \textsuperscript{29} Interview with IISS Officer 2, 10 May 2007, International Institute for Strategic Studies Headquarters, London, UK.
\item \textsuperscript{30} Exploitation Policy of the Dutch Military Intelligence and Security Service (MIVD). April 2006
\end{itemize}
\end{footnotesize}
for flexibility: a repeated offending of these rules by an intelligence service will almost immediately lead to a decrease in the reception of intelligence products from other national intelligence services.31

Bilateral and multilateral sharing

As was said before, the majority of information sharing within the European Union takes place on a bilateral or multilateral basis. Intelligence and security services and law enforcement agencies have many structured contacts with law enforcement agencies from other Member States within the European Union.32

All types of information are shared through these national – national contacts. There are some well-known networks, such as the exchange between the UK and Spain (they share a history of terrorism with the IRA and ETA) and the Benelux, the cooperation agreement between the Netherlands, Belgium and Luxemburg. Other relationships of sharing exist between the UK and France, the Scandinavian countries (including non-Member State Norway) and Spain and Italy.33 The goal of information exchange between intelligence services is always the improvement of their information position on a certain topic – intelligence cooperation in itself is generally not regarded as the target.34

National intelligence and security services are generally more hesitant towards European information cooperation than national police forces. However, national intelligence services emphasize that information needed to save lives (e.g. information about an imminent terrorist attack) will always be shared with the designated other Member State: no intelligence service will keep such information away from the target country.35 Thus, in case of urgent need, intelligence exchange will generally take place. This is emphasized by operational personnel to counter commonly heard critiques that “intelligence services only think about their own interest”.

32 Exploitation Policy of the Dutch Military Intelligence and Security Service (MIVD). April 2006
33 Interview with IISS Officer 2, 10 May 2007, International Institute for Strategic Studies Headquarters, London, UK.
34 Exploitation Policy of the Dutch Military Intelligence and Security Service (MIVD). April 2006
35 Interview with AIVD officer, 23 February 2007, AIVD headquarters, Leidschendam-Voorburg, the Netherlands.
Another way in which national intelligence and security services exchange information is through so-called peer evaluations or benchmarking. These peer evaluations consists of visits of delegation of one national intelligence and security service, visiting another national intelligence and security service. For instance, the Danish military intelligence service organizes a visit to the Greek military security service. During this visit, several types of information are exchanged, leading to advices in different areas and the exchange of best practices.36

Most importantly, national intelligence services report that the contacts amongst them are good and well organized. If necessary, national intelligence services encounter no problems in reaching each other when an urgent information exchange is needed. They emphasize that this exchange occurs frequently and without any hindrance or involvement by the European Union. They thus express a preference for maintaining the status quo of mostly bilateral contacts, without too much European involvement, because it is not regarded as required for cooperation at a bi- or multilateral level.37

One intelligence officer gave the following example to emphasize that European policy in counter-terrorism is often political, rather than operational:

Recently, the EU proposed to monitor the content of websites that might contain materials inciting religious violence: so-called “radicalization websites”. I think that they don’t have any idea what they are talking about. If you monitor websites, or even go so far as to close down certain websites, this information will pop up in ten other places. It’s like cutting off a dragon’s head: immediately five new heads will pop up. The people making EU counter-terrorism policy have no idea about what it is really like to fight terrorism – they are just making political gestures. The EU should not even concern itself with terrorism. They should not even want to have operational information – better leave that to the [national] intelligence services. Just because terrorism is trendy, the EU wants in. But they’re not competent. They should stay out.

This particular intelligence officer is evidently skeptical about European counter-terrorism involvement. Indeed, many national intelligence services consider that the added value of the EU to national counter-terrorism policy is inherently limited. Especially in the area of bilateral and multilateral exchange, national intelligence services express a preference for very limited European involvement.

36 Interview with AIVD officer, 23 February 2007, AIVD headquarters, Leidschendam-Voorburg, the Netherlands.
37 Ibid.
4.6 National – European sharing

This type of intelligence exchange refers to information exchanged or shared between a national intelligence/security service and a European information agency. For instance, information about an ongoing investigation about Albanian organized crime transmitted by German police to Europol could be classified as national – European information exchange. In the field of terrorism, the most important European information agencies are Europol and SitCen. Their role within the European intelligence community will be discussed later during this chapter.

Principles for European intelligence sharing

When it comes to sharing information with European agencies, national intelligence services often apply the same principle. A request is forwarded by a European agency (such as SitCen or Europol) and received by a national intelligence agency or law enforcement body, who usually has a designated point of contact for exchanges with European bodies. If an appropriate answer is directly available, e.g. in the form of a report, such information is usually forwarded rather expediently. However, if such information is not directly available, and the national service has to use resources to acquire such answers, a request for information by a European agency is usually not granted.38

National intelligence services have seen a growing role of European information bodies. European bodies have always played a role in crisis management operations (such as after natural disasters etc.), but they are becoming increasingly important for counter-terrorism policy as well, as cooperation between them has increased.39

The default point of contact between national intelligence services and EU agencies are the national senior representatives or permanent representatives of Member States that are stationed with the European agencies such as NATO or the EU Commission. They are referred to by different names: national

---

38 Interview with AIVD officer, 23 February 2007, AIVD headquarters, Leidschendam-Voorburg, the Netherlands.
senior representatives, permanent representatives, senior liaison officers, etc. These senior national representatives can also forward requests from European agencies to national intelligence services.  

The following section discusses the role and position of these different European information agencies and the nature of sharing in the European intelligence community between them and national intelligence services.

## 4.7 The Joint Situation Center (SitCen)

### Introduction

The Joint Situation Center (SitCen) is located within the General Secretariat of the Council, and produces so-called external intelligence for the EU’s Second Pillar. Its function is to produce intelligence analyses in order to support EU policy making. The SitCen monitors and assesses events and situations worldwide on a 24-hour basis with a focus on potential crisis regions, terrorism and WMD proliferation.  

The SitCen (housed in the Justus Lipsius building in Brussels) is the point where different types of national intelligence and ‘civil’ information are synthesized to all-source assessments and external intelligence. SitCen is responsible for providing EU decision makers working on the Common Foreign and Security Policy (CFSP) in the Second pillar with relevant intelligence. It started its work in February of 2002. It produces, on average, 100 intelligence products per year, 40% of which deals with terrorism. SitCen provides the Council of the EU with strategic intelligence-based assessments upon counter-terrorism matters. It began its work soon after 9/11 (2001) but did not begin to deal with internal security policy until after the Madrid bombings in March 2004.

---

40 Exploitation Policy of the Dutch Military Intelligence and Security Service (MIVD). April 2006  
42 Building a European Intelligence Community in response to Terrorism, Muller-Wille, B. European Security Review, no. 22, 1 April 2003,  
The SitCen is located within the General Secretariat of the Council, and is mainly tasked by the High Representative. The High Representative also appoints the Director. Currently, the Director is William Shapcott (UK), and the British have been amongst the first to realize that the EU High Representative needed credible intelligence support in the form of an EU external intelligence agency.44

The SitCen provides tailored situation and threat assessments, based on national intelligence, open source, diplomatic reports from Member States and the Commission’s representations. Its Counter-Terrorism (CT) Unit complements this by making threat assessments specifically regarding terrorism. The products from SitCen primarily support the SGHR of CFSP, Solana, and the national ambassadors that comprise the Political and Security Committee, the Union’s principal decision-making body in the area of European Security and Defense Policy (ESDP).45

Furthermore, SitCen renders intelligence support to the Policy Planning and Early Warning Unit, or Policy Unit. The Policy Unit considers policy options stemming from SitCen material as well as national diplomats. The Policy Unit was created in October 1999 at the same time as the High Representative for CFSP, to whom it reports. It provides the High Representative with assessments of the Union’s interests pertaining to CFSP, early warning and draft paper setting out the various policy options.46

The SitCen is comprised of three units:

- Civilian Intelligence Cell (CIC), which provides political and counter-terrorism assessments
- General Operations Unit, which provides continues operational support, research and non-intelligence analysis
- Communications Unit, which handles communication security and runs the Council’s communications center (ComCen).

45 Building a European Intelligence Community in response to Terrorism, Muller-Wille, B. European Security Review, no. 22, 01-Apr-03,
Chapter 4

Tasks and modus operandi

The SitCen generally keeps a very low public profile. For instance, no website is available for this EU information agency, nor does it grant regular interviews to students, researchers or other interested audiences. Public appearances by its Director are infrequent. The low public profile of SitCen is deliberate and has a number of causal factors contributing to it. Most importantly, SitCen has “bent over backwards” to earn the trust of its contributors, the intelligence and security services of its Member States. Everything is based on the principle of trust and confidence. Apparently, SitCen believed it could earn the trust of national intelligence services with such a low public profile.

However, all across the EU, national and European intelligence services are being pushed for more openness and transparency. SitCen is also responding to this development and is considering being more open because it needs support from parliaments, mostly at the national level, but also the support of the EP. Nevertheless, the relationship between SitCen and the European parliament will remain problematic, since the intelligence services of Member States do not support this relationship with much enthusiasm – they remain preoccupied with the classified nature of the intelligence that is shared between their intelligence services and SitCen.

SitCen’s work is aimed at developing resistance within the EU towards terrorist attacks. Overall, SitCen is supposed to provide the Council with strategic intelligence-based assessments on counter-terrorism matters. It is well understood that no intelligence service can prevent all terrorist attacks in the near future hence its focus is on building resistance. As the EU builds defenses against terrorist attacks, SitCen can assist by rendering strategic advice, for instance on aviation security, the use of the Internet, and radicalization. It helps the EU in designing measures for its counter-terrorism policy. The use of SitCen intelligence helps to support EU policy, which is working especially well in the Third Pillar instruments.

49 Interview with Officer of the Joint Situation Center. General Secretariat, Brussels, 16 April 2007.
Currently, SitCen employs 25 analysts, who are so-called ‘double-hatted’: this means that they function as a representative of their own national intelligence service on the one hand, and as a SitCen analyst on the other. Not all Member States are represented in SitCen: however, all Member States contribute intelligence to its work. SitCen’s work, designed to cover global threats, focuses on three main areas:

- Intelligence support to EU missions; risk assessments
- Geographical areas outside the EU (for instance, the Great Lakes area in Africa)
- Terrorism inside and outside the EU (for instance, radicalization)

The SitCen products are distributed to clients and decision makers in the Second (Common Foreign and Security Policy) and Third (Police and Judicial Cooperation and Criminal Matters) Pillar.

The SitCen mandate explicitly concerns only strategic information. However, especially for its task of rendering intelligence support to EU crisis management missions, it regularly needs operational information as well. It is quite successful in receiving operational information from national civil and military intelligence services, since the Member States realize that it is done to protect their own soldiers on these missions.

Mostly, SitCen works with point-to-point contacts with the Member States. This means that information is exchanged bilaterally, between one Member State and its representative to SitCen. SitCen does not have a secure communication system with the Member States. So they use the secure communication system of the CTG in the Council where necessary. This secure communication system, the name of which is classified, can be compartmentalized. This means that parts of the communication system can be separated from the main communication system. This provides an extra-secure environment for bilateral or multilateral exchanges.
SitCen in the European intelligence community

Both the Intelligence Division of the EU Military Staff (INTDIV) and SitCen produce so-called external intelligence for the Second Pillar of the EU, with the difference that INTDIV produces military intelligence, and SitCen focuses on civil intelligence. To create more synergy between the two bodies, INTDIV and SitCen products are now regularly combined under the header of SIAC, or Single Intelligence Analysis Capacity. SIAC is a form of reporting that merges the products from SitCen and the INTDIV. This SIAC product is then distributed to the intelligence customers, mostly the Council. The added value of SIAC is that it forms a single stream of reporting, thus providing more consistent intelligence support to European decision makers. Differences between civil and military intelligence are decreasing at the national level; and this development is also slowly becoming visible at the European level through the emergence of SIAC.

In terms of external intelligence, the Council has maintained a strict division between military and civil external intelligence, despite the fact that the distinction between civil and military intelligence is becoming blurred. All civil external intelligence is collected and processed by SitCen; all military external intelligence passes through the Intelligence Division of the European Union Military Staff. However, the new SIAC intelligence products are unifying this divide.

SitCen is seen within the Council as the leading EU agency in the area of terrorism. SitCen itself also acknowledges the central role it has within the EU’s counter-terrorism strategy. However, according to SitCen, the Council and the Commission still do not fully understand the threat of terrorism to the European area of justice, liberty and security. It argues that “the consequences of terrorism have not yet been large enough for Europe to take serious steps against it.”

50 Interview with Officer of the Intelligence Division (INTDIV) of the European Union Military Staff. EU Military Staff Headquarters, Brussels. 12 April 2007.
51 Interview with Officer of the Joint Situation Center. General Secretariat, Brussels, 16 April 2007.
52 Ibid.
53 Interview with Officer of the Intelligence Division (INTDIV) of the European Union Military Staff. EU Military Staff Headquarters, Brussels. 12 April 2007.
54 Interview with Officer of the Joint Situation Center. General Secretariat, Brussels, 16 April 2007.
The SitCen produces for many customers but no explicit rules exist as to who can task the agency. A large client was the office of the “counter-terrorism czar” Gijs de Vries, who tasked SitCen. Many other bodies also receive SitCen products: the Council, the High Representative, the Commission, the Presidency, several working groups (such as the working group on terrorism) and senior EU officials. Member States can also task SitCen by requesting an intelligence report on a specific topic. However, such reports are consequently made available to all Member States – SitCen does not report bilaterally to Member States. Thus, the tasking of SitCen is both formal and informal, and is not generally covered by strict rules of a statute.

The relationship between SitCen and the Commission can be further improved. The Commission has not always been “intel-minded”, but is increasingly realizing the importance of intelligence and intelligence-led law enforcement. Several Member States have expressed a preference for a stronger link between SitCen and the Commission, and an improvement of information flow. The Commission now shared information with SitCen on a routine basis, focusing on the Commission’s secure ‘crisis room’.55

4.8 Sharing with SitCen

National intelligence service interviewees report a good working relationship with SitCen. For instance, the Dutch Civil Security and Intelligence Service (AIVD) has seconded an analyst to SitCen. This AIVD employee works fulltime at SitCen in Brussels. Both parties report that a substantial amount of information is shared through this channel.

SitCen’s explicit mandate for strategic information confirms the trend that in the Second Pillar of foreign and security policy, the EU is mostly concerned with strategic counter-terrorism information: how networks work, how they are financed and organized, their ideologies and potential targets.56 However, with ever greater interaction between the Second and Third Pillar of the EU, the difference between strategic and operational intelligence is likely to shrink. The use of intelligence to combat terrorism by definition implies the use of operational and personal data. It is to be seen whether SitCen’s mandate will

---

be expanded to enable more effective counter-terrorism intelligence gathering, specifically expanding its mandate to include operational intelligence. Their operational significance is very limited, since SitCen does not have a mandate for operational information.

Information flow between SitCen and national intelligence and security services is greatly improved when the national intelligence service sends one of their officers to SitCen. Understandably, this improves the information position of both the national intelligence service and SitCen. Furthermore, the personal contacts between the seconded national officer and other national officers at SitCen can aid international intelligence cooperation in other European forums, as well as bilaterally. This is an example of how personal contacts can aid intelligence cooperation on different levels.

Various national intelligence services report regular contacts with SitCen. Furthermore, SitCen has a rather substantial rate of production – circa 100 reports or threat assessments a year. SitCen does receive classified information from Member States, including operational information – however, this information usually has been ‘cleaned’, whereby the sources and personal data have been removed. This is done in order to be able to guarantee source protection, an essential principle in the intelligence community.

Moreover, national intelligence services do not yet completely trust SitCen’s ability to handle the classified document of all European information agencies and especially, of the newer EU Member States who are indirectly able to access such information. The future of SitCen will likely see a clarification of its mandate, specifically about who can task the agency. However, the agency is still in its childhood, and is only starting to develop an institutional culture.

---

58 Interview with AIVD officer, 23 February 2007, AIVD headquarters, Leidschendam-Voorburg, the Netherlands.
59 Ibid.
60 Ibid.
61 Ibid.
62 Ibid.
63 Ibid.
Significance of SitCen products

Various interviewees emphasize the importance of SitCen reports and assessments, especially for newer Member States. For Member States with experience with terrorism, such as the UK, Spain, but also Germany and the Netherlands, SitCen products are useful for filling in gaps in their information position. Occasionally, a SitCen product provides information that these intelligence services did not previously possess, and thereby adding value.

However, newer Member States such as Poland and Slovenia have little experience with terrorism in all forms, especially Islamic terrorism. For them, SitCen products provide a wealth of information, which would be costly and lengthy for their own intelligence and security services to collect. Therefore, the average value of a SitCen product for the intelligence and security services of these new Member States is relatively large.

4.9 European Police Organization (Europol)

Introduction

This European Police Organization sits at the EU’s heart of exchange of criminal intelligence. One of its principal tasks is facilitating the exchange of information between the EU Member States. Europol is a police organization, and not an intelligence service. It does not have power of arrest or prosecution. Besides Europol, police cooperation is especially intensive among the so-called Schengen countries in the form of the Schengen Information System (SIS), the Supplementary Information Request at the National Entry (SIRENE) and cross-border supervision.

64 Interview with IISS Officer 2, 10 May 2007, International Institute for Strategic Studies Headquarters, London, UK.
66 Ibid.
Legal framework and mandate

The legal framework of Europol consists of several international treaties, namely the Europol Convention, the Protocol on immunities of Europol officers and the Protocol on the interpretation of the Europol Convention by the European Court of Justice (ECJ). Europol’s counter-terrorism task, as quoted from the Europol Convention, states that “the objective of Europol shall be, within the framework of cooperation between the Member States...to improve, by means of the measures referred to in this Convention, the effectiveness and the cooperation of the competent authorities in the Member States and preventing and combating terrorism.”

Furthermore it should be added that the legal framework of Europol is based outside the EU treaties. Several Members of the European Parliament have suggested that this should be changed, thus increasing the accountability of the European Police Organization.

After numerous enlargements of its mandate, Europol is now competent to investigate murder, kidnapping, hostage-taking, racism, corruption, unlawful drug trafficking, illegal immigrant smuggling, trade in human beings, motor vehicle crime, all forms of serious organized crime and terrorism. The Council has decided to set up a team of counter-terrorist specialists with the task of collecting and analyzing data concerning current threats and providing operational and strategic analyses within Europol.

Liaison officers from Member States

All EU Member states have seconded liaison officers to the Europol Headquarters in The Hague, the Netherlands. The liaison officers posted at Europol were installed after a joint action decision by the EU in 1996. Their function is specifically to focus on information gathering and exchange. They are to “facilitate and expedite the collection and exchange of information through direct contact with law enforcement agencies and other competent authorities in the host State”, and “contribute to the collection and exchange

67 Europol Convention, article 2.
The European intelligence community

of information, particularly of a strategic nature, which may be used for the
improved adjustment of measures” to combat international crime, including
organized crime and terrorism. Over 300 liaison officers have been posted
by EU countries, and they work in close cooperation with each other.

Although these liaison officers in themselves do not constitute formal
arrangements for information sharing, their contacts are essential in any
intelligence sharing. Personal relationships with other liaison officers greatly
facilitate the exchange of intelligence or other types of information. They act
as hubs or facilitators within all sorts of informal networks of intelligence
sharing in this context.

Some analysts argue that the EU has made little progress in coordinating
and enforcing measures involving intelligence swapping and police
coordination. However, through Europol, an extensive network of liaison
officers has been created. As was argued before, these liaison officers form
the heart of both formal and informal channels of information sharing, and
are therefore essential to intelligence exchange in the European Union. The
implementation of the availability principle is likely to further develop this
exchange of information.

Joint Investigation Teams (JIT)

An important element of Europol’s role as the EU’s criminal intelligence body
is to set up Joint Investigation Teams (JITs). The JITs will be integrated into the
Europol Convention. The main purpose of these Joint Investigation Teams is
to carry out investigations for a specific purpose and limited duration in one
or more Member states, in a combined effort with national police forces. Both
national law enforcement personnel and Europol officers take place in such
Joint Investigation Teams. The setting up of these joint investigation tams
has been argued to be the most important improvement to Europol’s mandate.
Although the role of Europol in the investigation teams can be described as
‘support capacity’, “this should not obscure the fact that Europol can be of
considerable importance for the joint investigations teams. In particular,
Europol can play an important role in supplying and bringing together vital
information stemming from the different Member States.”

71 Ibid.
72 Amongst others: Block, L. (2005) European Counter-Terrorism Culture and
Methodology, TerrorismMonitor, Volume 3, issue 8, 21-Apr-05.
74 Ibid, p. 263.
These investigation teams function within a strict legal framework, and are comprised of investigators from different Member States and Europol experts. The work of these investigation teams often leads to so-called “high impact operations”, where larger networks of organized crime are being investigated and disrupted across Member States’ borders. However, their effectiveness can be limited because of political considerations.75

Europol is more than merely an intelligence broker, since it also compiles and analyses information from several states. However, Europol has no executive authority, so Member States must voluntarily submit intelligence to Europol. Europol is the European Law Enforcement Organization which aims at improving the effectiveness and co-operation of the competent authorities in the Member States in preventing and combating terrorism, unlawful drug trafficking and other serious forms of international organized crime.

4.10 Sharing with Europol

Europol works with a system of National Units. These national units are designated contact points within national police forces. Europol works as a police organization so they generally do not have information exchange contacts with national intelligence and security services. If necessary, they can receive information from national intelligence and security services through national law enforcement agencies, or other European information agencies such as SitCen. The AIVD, for instance, reports no direct contacts with Europol – they are managed by the Dutch national police (KLPD), which forms the National Unit (point of contact with Europol).76

Furthermore, intelligence services are hesitant about the role of Europol as a European pool77 of counter-terrorism intelligence. They concur that European cooperation is important to ensure the security of European citizens, but are very hesitant to allow European interference with their mandate. Most

76 Interview with AIVD officer, 23 February 2007, AIVD headquarters, Leidschendam-Voorburg, the Netherlands.
77 The words “pool” and “clearing house” are used interchangeably throughout this chapter. The terms refers to a role of Europol as the central hub amongst many relationships of intelligence sharing within the EU. In this role, all MS would submit all relevant intelligence to Europol. Europol would analyse and verify the intelligence, and distribute it amongst the relevant parties.
importantly, they do not want to be forced to submit intelligence to a European agency. They see SitCen and Europol as a good platform, a useful forum to meet other intelligence officers and to receive updates about ongoing European investigations.

**Europol’s tasks**

Europol plays a central role within the counter-terrorism field in the EU. Europol functions a center of expertise: it facilitates and stimulates information exchange between Member States and between Member States and Europol through a secure digital network. In this sense, Europol presents an extra resource for Member States: an extra source of information, and a possible source of analytical and operational assistance. Europol also provides language support in the form of translations, which are done at Europol headquarters.

Europol works with a system of Analytical Work Files (AWF): currently Europol has 17 Analytical Work Files ongoing, functioning within the Europol legal framework, mainly consisting of the Europol Convention. Through the Analytical Work Files, Europol can establish operational and analytical support to ongoing criminal investigations within Member States. Europol deals with various kinds of organized crime and terrorism, and received all its information from the Member States, since it does not have the mandate to gather information or conduct investigations.78

Europol’s Counter-Terrorism Unit considers OSINT as an important source of information and has made OSINT part of the intelligence cycle. A dedicated team monitors and processes OSINT to support other CT activities. OSINT analysis is used for Europol’s work on terrorism, and monitors the security environment. Intelligence is largely based on OSINT – this section can have added value for many Member States. Collecting OSINT is a costly and time-consuming job. The OSINT gathered by Europol can augment the research and material available in Member States.79 Effective OSINT exploitation helps to put information from the Analytical Work Files into perspective and to develop more future oriented strategic and tactical assessments.

---


79 Interview with Europol Officer 2. 27 February 2007, Europol Headquarters, The Hague.
All Europol products (usually in the form of assistance in an ongoing criminal investigation) are produced in close dialogue with the requesting Member State. Information from an ongoing investigation, for instance in Spain, can be cross-referenced by Europol with information on the same topic in other Member States. Much of the dialogue is conducted with the help of liaison officers: seconded police officers from national police forces, stationed at Europol headquarters. The liaison officers are always informed about ongoing assistance from Europol to their Member State; similarly, the National Units within the concerned Member State are always involved.80

When it comes to combating organized crime, Europol can provide analytical and operational support to Member States when they request such support. This is an especially valuable resource for smaller Member States, such as Slovenia and Portugal. Their ongoing investigations can greatly benefit from a European viewpoint, and Europol is the designated actor to provide this. In Europol’s opinion, however, larger Member States could benefit from Europol as well. Some networks of organized crime can only be discovered when one ‘zooms out’, and looks at it from a European perspective. Freedom of movement within the EU and Schengen is exploited by groups of organized crime and terrorist groups. Investigations tend to be transnational and complex, which is why Europol can provide added value.

As Europol is completely dependent on the information from Member States, its work can only be as good as the best information it receives. In the past, there have been problems in the cooperation between Europol and the Member States. If Europol does not receive current or high-quality information, the Europol product such as the EU Terrorism Situation and Trend Report (TE-SAT) will not have much added value for the Member States. However, Europol reports that more and more Member States ‘understand’ Europol: meaning that these Member States understand the added value that Europol can provide, and thus feed them with good criminal intelligence. As a result, Europol’s products have increasing value for the Member States.81

Eurojust (the European Union Judicial Cooperation Unit) is often a partner in Joint Investigations Teams. Eurojust assists EU Member States in judicial proceedings, and legal investigations. Eurojust reports good cooperation with Europol, both in- and outside the Joint Investigation Teams.

81 Ibid.
Handling codes

The Analytical Work Files used by Europol protect the ownership of the data by so-called handling codes. These handling codes are tagged to the information, and contain instructions by the provider of the information on how this information can be used. For instance, a handling code can contain the limitation that some information cannot be used in courts. Another example is a handling code that explicitly provides that the provider of the information must be consulted before information can be shared. Through the process of the Analytical Work Files and the handling codes, Europol protects the ownership of the data, respects the rules of data protection and can provide added value for the Member States.82

National Units

The most crucial actors in determining the value of Europol are the National Units: national contact points within national police forces who manage the contacts with Europol. These National Units are in charge of “selling” Europol to their Member State: convincing them of Europol’s added value in sharing intelligence, and convincing the Member State to feed Europol with good intelligence. Therefore, the success of these National Units is crucial to the success of Europol. Member States are increasingly realizing that Europol is a valuable resource, and a tool that can aid their own investigation.83

One of Europol’s most important tools is Council Decision 2005/671/JHA (20 September 2005).84 This decision stipulates that Member States are obliged to transmit information concerning terrorist crimes to Europol. Understandably, Europol would benefit the most from early access to such information. However, not all information concerning terrorist crimes is submitted from Member States to Europol. Europol could be more helpful, both for Member States and for European decision makers, if JHA 671 would be more strictly adhered to. Europol could also do more with the present resources if Member States would comply with JHA 671.

---

Europol as a clearing house of information

In ongoing criminal investigations, Europol can provide the most added value when it is involved at the beginning of the investigation. When patterns of organized crime are not yet visible to a national police force, they sometimes can be visible for Europol. However, the case of terrorism is different. When a Member State is trying to prevent a terrorist attack from occurring, these investigations are usually being carried out by intelligence and security services, rather than by police. Once a terrorism case arrives at the desk of the police, it is usually a rather advanced investigation: for instance, when they are ready to make an arrest. 85

Europol is not often involved with intelligence and security services. Its contacts are with national police forces, and the organization was not designed as a European intelligence clearing house (i.e. a collection point where all relevant information on a topic is stored, analyzed, and distributed). Therefore, Europol might have more added value in fighting organized crime than in fighting terrorism. The increasing links between organized crime and terrorism (such as money laundering) could however augment Europol’s role as a counter-terrorism body.

The role of Europol as a clearing house is a point of discussion both inside and outside Europol. However, the long runtime of most Analytical Work Files causes Europol to play the role of clearing house nonetheless. Especially the Analytical Work File on terrorism, running since 1999, holds valuable information concerning trends and past attacks, which can provide useful insights for new counter-terrorism policy.

One of the problems hindering Europol to act as a European clearing house of criminal intelligence, is the lack of resources. Europol officers report a lack of analysts, and therefore a need to be very selective in which investigation to aid one or the other Member State with. 86 With more resources, Europol says it would also be more capable of fulfilling the ‘clearing house’ role that was mentioned before.

In the eyes of Europol and the Council, there exists no doubt that Europol should fulfill this role of clearing house and “intelligence broker” within the EU. However, the problem is the political will of Member States to submit and share their sensitive intelligence with Europol on all topics. In the eyes of the

---

86 Ibid.
Europol interviewees, Europol has been gaining a lot of confidence over the last few years. It is seen as a good sign that Europol is now receiving more information than they can handle with present resources. Member States who have ‘tested’ Europol services have been content, and will increase their cooperation and information flow in the future. It works as a process of building of trust: once positive results have been achieved, Member States are more likely to work with Europol again. If Europol analysis has real added value for Member States, there is more political will to increase information flow towards Europol.87

Europol’s changing role

Europol is developing more and more into a true EU level institution catering to the EU policy makers. Europol can identify trends and patterns within certain policy areas, which individual Member States are not able to see. Therefore, Europol could provide the EU (both in the Second and the Third pillar) with valuable information in the counter-terrorism area. Europol is becoming increasingly strategic, and provides more forward-looking assessments, instead of just being an extra investigator for Member States’ police forces.88

Europol is increasingly thinking bigger, and realizing the pivotal role it can play at the EU level. Notwithstanding, Europol should continue to cater to its most important customers: the national police forces. However, the mentality of Europol is changing. Europol is increasingly aspiring to be an information and service provider for the Member States and for the European Union. This concerns a higher-level and more ambitious role: Europol as the criminal intelligence center within and for the European Union.

Data protection

Although data protection has explicitly been excluded as a topic of this research (see chapter 1), it is necessary to say a few words on the data protection of the European citizen in relation to the work of Europol. Europol’s work and the Analytical Work Files are governed by strict data protection rules as laid down in the Europol Convention. Personal information contained in work files can be stored for a maximum of 3 years. Europol’s work is overseen by the Joint

Supervisory Body, composed of data protection officers from the Member States. The Analytical Work Files are designed as temporary entities to protect the privacy of the suspects. However, this leads to hindrance when it comes to identifying trends and threats. The opening order of the Analytical Work Files is strictly governed.

Europol’s future

To conclude, Europol has many tasks to perform within the European intelligence community. Firstly, it acts as a facilitator for European information exchange. This is done through its secure communication network, the liaison officers and the National Units. Secondly, Europol aids Member states, by helping them with ongoing investigations, by their analyses and threat assessments, by the use of the Joint Investigation Teams, and by providing several translating services. Thirdly, Europol acts as a center of excellence and expertise. By providing a unique European viewpoint, Europol can provide real added value to the ongoing investigations within Member States. Fourthly, Europol should provide intelligence support to EU decision makers in the Second and Third Pillar. The information contained in the Europol Analytical Work Files is a valuable source, both for Member States as well as for the EU in intelligence sharing. The possibly increasing role of clearing house also falls under this task and will be discussed below.

4.11 The European Union Satellite Center (EUSC)

Introduction

The European Union Satellite Center is located in Torrejón de Ardoz, Spain. Its mission is to support the decision-making capacity of the European Union by providing analyses of satellite imagery and collateral data. Its institutional position is within the Council of the European Union, and it is staffed by image analysts, geospatial analysts and supporting personnel. The Center supports the decision-making of the European Union in the field of the Common Foreign and Security Policy (CFSP), in particular of the European Security and Defense Policy (ESDP), including European Union crisis management.
The European intelligence community

operations, by providing, as appropriate, products resulting from the analysis of satellite imagery and collateral data, including aerial imagery, and related services. The EU Satellite Center assures technical development activities in direct support to its operational activities, as well as specialized training for its image analysts, including external participants from Member States and third states. The EUSC works closely with the European Defense Agency (EDA) and the European Maritime Safety agency (EMSA).

The EUSC is tasked by the Secretary-General/High Representative of the EU and purchases commercial imagery and obtains from French, Spanish and Italian satellites. After, it analyses this imagery for ESDP/CFSP structure within the Council, the Commission, Member States and third states or international organizations.

Mandate and tasks

The Satellite Center’s areas of priority reflect the key security concerns defined by the European Security Strategy, such as monitoring regional conflicts, state failure, organized crime, terrorism and proliferation of weapons of mass destruction. The EUSC gives, for example, support to EU deployed operations such as the EUFOR in Bosnia and Herzegovina, humanitarian aid missions and peacekeeping missions. The Center is also an important Early Warning tool, facilitating information for early detection and possible prevention of armed conflicts and humanitarian crises. The Center carries out tasks in support of activities such as general security surveillance over areas of interest, the Petersburg type tasks, support to humanitarian and rescue tasks, support to peacekeeping tasks, tasks of combat forces in crisis management, including peacemaking, treaty verification, contingency planning, arms and proliferation control (including weapons of mass destruction). It supports UN missions, such as peacekeeping and humanitarian operations in the Democratic Republic of Congo and in Sudan.

Chapter 4

4.12 The Intelligence Division of the EU Military Staff (INTDIV)

Introduction

The INTDIV EUMS is the intelligence division of the EU Military Staff (EUMS). The EUMS was established in January 2001 to provide military expertise and support to the European Security and Defense Policy as well as to conduct EU-led crisis management operations. It is the focal point for the exchange of military intelligence at the European level and is comprised of around 30 seconded officers from national military intelligence agencies. It assesses and synthesizes intelligence from various sources with the overall objective of supporting decisions made in the ESDP context. Its intelligence clients include the Director-General of the EUMS, the High Representative, the EU Military Committee, SitCen and appropriate national intelligence agencies.93

The EUMS is a permanent body since 11 June 2001, and is tasked by the EU Military Committee, representing the Chiefs of Defense of all Member States of the EU. The EUMS provides in-house military expertise for the Secretary-General/High Representative. The main operational functions of the EUMS are early warning, situation assessment, and strategic planning.94 Comparable to SitCen, the added value of INTDIV lies in its ability to assemble and make available analysis in the context of ESDP.95

Mandate and tasks

The Intelligence Division (INTDIV) provides the EUMS with strategic intelligence planning, requirements and procedures, including early warning and situation assessment. The INTDIV is the focal point for the exchange of military intelligence at the Union level. It receives its information from national military intelligence services.96 INTDIV compiles reports, based on national intelligence, to support the strategic planning that starts as soon as

94 European Union Military Staff Brochure: Providing Military Capabilities to the EU.
a crisis emerges and ends when the EU political authorities approve a military strategic option or a set of military strategic options. The EU has military crisis management operations in Bosnia and Herzegovina, Macedonia, Moldova and Ukraine, the Democratic Republic of the Congo, Sudan (Darfur), Iraq, the Palestinian Territories, and Indonesia (Aceh). EU military operations have so far relied on national intelligence services for their intelligence function. The INTDIV adds to the work of national intelligence services.

The increasing number of EU-led crisis management operations is one of the most important arguments for better intelligence support to EU decision makers. No crisis management operation can be run without adequate intelligence support. The argument that peacekeeping and other forms of crisis management operations need to be adequately intel-supported is so prevalent, that even the UN –an ardent opponent of intelligence within its own organization- has at some point considered the establishment of an intelligence function to support its peacekeeping missions.

### 4.13 Other bilateral and multilateral initiatives

#### Multilateral Initiatives

There are and were other, multilateral initiatives of EU Member States that share intelligence. The most important ones are and were:

- the Trevi group (Terrorisme, Radicalisme, Extrémisme en Violence Internationale) consists of the Ministers of Justice and Interior of the EU. Its functions have been taken over by the Third Pillar of the EU.

---

97 Muller-Wille, B. (2003) Building a European Intelligence Community in response to Terrorism, European Security Review, no. 22, 01-Apr-03,
EU. The Trevi group was largely an intergovernmental forum for collaboration outside of the formal treaty structure and it lacked a permanent secretariat, but it provided the law enforcement authorities of the European Community with a useful way to communicate and exchange information and best practices.

Berne Club (1971) consists of 18 countries. Its framework of thematic meetings is based on concerns of the day. Informal contacts take place between small groups, often compartmentalized. The Club of Berne, as it is also called, is an important forum for national intelligence services and is reported to play a crucial role in many bi- and multilateral national contacts.

Kilowatt Group (1977) is outdated and now little more than a telex network.

**Police Chiefs Task Force and the Police Working Group on Terrorism**

These groups consist of police chiefs from all EU Member States, and are international fora to help high-level national police officials share best practices and information on current trends in cross-border crime, and contribute to the planning of joint operations.

### 4.14 European – European sharing

This type of information exchange occurs between European information agencies. For instance, if the EUSC transmits satellite imagery to SitCen to aid the organization of humanitarian support after a natural disaster in Asia, this exchange can be classified as European – European. In the field of terrorism, the most important European – European exchanges occur between SitCen and Europol. Europol receives the threat assessments compiled by SitCen.

---


103 Interview with IISS Officer 2, 10 May 2007, International Institute for Strategic Studies Headquarters, London, UK.
The European intelligence community

containing strategic information about the security situation inside and outside the European Union. Other European – European exchanges are outlined below.

Europol - INTDIV

Europol reports no cooperation with INTDIV. However, such cooperation is desired in the future.104

Europol - EUSC

Europol reports no cooperation with EUSC. However, such cooperation is again desired in the future.105

SitCen - INTDIV

The intelligence division of the EU Military Staff and the Joint Situation Center are housed in the same building in Brussels. This enables a good deal of cooperation between these two agencies. In general, SitCen provides civil, strategic assessments. The INTDIV focuses on military-tactical and military-operational information. Occasionally, they produce military-strategic information as well. The merging of the products of these two agencies has been taking place since the founding of these organizations, on a modest scale. Lately, a more systematic approach has been initiated. INTDIV and SitCen products are now regularly combined under the header of SIAC, or Single Intelligence Analysis Capacity. SIAC is a form of reporting that merges the products from SitCen and the INTDIV. This SIAC product is then distributed to the intelligence customers, mostly the Council.106

SitCen - EUSC

SitCen reports a good working relationship with the EUSC. They use the EUSC products (mostly satellite imagery) for long-term monitoring of sites of interest, such as nuclear production facilities in North Korea. A secure communication

105 Ibid.
106 Interview with Officer of the Intelligence Division (INTDIV) of the European Union Military Staff. EU Military Staff Headquarters, Brussels. 12 April 2007.
system is in use between SitCen and the EUSC. However, there are also limitations to EUSC products for SitCen. As was described before, the EUSC has no own collection capabilities: it buys commercial imagery and receives IMINT from EU Member States. However, its imagery is used frequently in SitCen products.

SitCen and Europol

Both SitCen and Europol are being called the EU’s counter-terrorism agency. This immediately begs the question of how the two agencies interact and cooperate, and to what extent their mandates overlap. The first and foremost difference between Europol and SitCen is that the former is a police organization, while the latter is an intelligence agency. This difference is crucial in mandate and tasks, as has been explained throughout this study. This entails, for instance, a difference regarding the moment in time where the organizations exercise their powers.

SitCen, being an intelligence agency, conducts its investigations preferably before an attack takes place (pre). Europol, being a police organization, usually performs its tasks after an attack takes place (post). They perform their tasks in different ways, and sometimes this creates problems for joint products. However, the relationship between Europol and SitCen has greatly improved and is currently providing added value for both organizations. Sometimes, joint reports are issues, and there are regular contributions of the organizations to the work of the other. SitCen appreciates the analytical work of Europol, and similarly, almost all SitCen products are forwarded to Europol, with the consent of the Member States.

Europol and SitCen do not yet share a secure communication system. All information exchange is currently executed with the assistance of couriers between The Hague (Europol) and Brussels (SitCen). 107

Europol and SitCen have an administrative and strategic agreement about the sharing of their products; this exchange takes place on a fairly regular basis. The two European information bodies exchange all types of information, but mainly threat assessments. SitCen informs Europol about their topics of

107 Interview with Officer of the Joint Situation Center. General Secretariat, Brussels, 16 April 2007.
interest, and the possible contribution Europol can give to these projects. The two directors (William Shapcott of SitCen and Max-Peter Ratzel of Europol) are in contact on a regular basis.\textsuperscript{108}

In terms of mandate, both SitCen and Europol are the central European agencies in the fight against terrorism. Both are called “leading EU entity in the fight against terrorism”, albeit in different pillars. The SitCen products are mainly, but not exclusively used in the Second Pillar. Europol products are distributed mainly within the Third Pillar. This entails differences in customers: Europol caters to national police forces, whereas SitCen distributes and receives mostly from national intelligence services.

It does not seem likely that EU counter-terrorism policy will be located within one EU pillar in the near future. Therefore, the law enforcement and intelligence support for counter-terrorism policy will continue to be provided by both SitCen and Europol. The Council and Commission can benefit from validated intelligence from two sources.

\section{4.15 The Prüm Treaty}

\textbf{Introduction}

The Prüm Treaty deserves a separate section within any mapping of the European intelligence community. The aim of the Prüm Treaty was to help the signatories improve information sharing for the purpose of preventing and combating the crimes of terrorism, cross-border crime and illegal migration. Current signatories of this treaty are Austria, Belgium, France, Germany, Luxembourg, Netherlands and Spain. EU Member States intending to join are Finland, Italy, Portugal, and Slovenia.

The original idea of Prüm was presented by the former German Minister of Home Affairs, Otto Shily, on 25 February 2005, during the inauguration of the \textit{Commissariat Commun de Police} in Luxembourg.\textsuperscript{109} The status of Prüm

\textsuperscript{108} Interview with Europol Officer 2. 27 February 2007, Europol Headquarters, The Hague.

as of yet is that of an international treaty, signed by seven Member States. It aims at “stepping up their cooperation, in order to combat terrorism, cross-border crime and illegal migration more effectively.” In this respect, the provisions of Prüm enable the exchange of very sensitive data, such as DNA and fingerprints.

The treaty is often described by its supporters as a concrete step to improve European integration in the field of law enforcement information exchange. As of yet, the Prüm Treaty is a multilateral treaty that functions outside the EU framework. However, efforts are ongoing to integrate the treaty into the EU framework, and to use it as a European-wide tool to further police cooperation and data exchange. However, if Prüm is to function completely within the European framework, its provisions will have to be made fully compatible with the aforementioned principle of availability.

4.16 Conclusion

This chapter aimed to introduce and map the European intelligence community, which fulfills the role of European intelligence function. This European intelligence function provides counter-terrorism intelligence support to EU decision makers in the Second and Third Pillar. The European intelligence community consists of many actors: European information agencies, (INTDIV EUMS, SitCen, Europol, and EUSC) but also the Council, the Commission, various bi- and multilateral working groups on counter-terrorism, Eurojust, the World Customs Organization, Interpol, CEPOL, the Task Force Chiefs of Police and Frontex.

110 Preamble of Council of the European Union, Prüm Convention, doc. 10900/05 CRIMORG 65 ENFOPOL 85, Brussels, 7 July 2005.
113 Den Boer, M. (2007) The growing convergence between “vertical and horizontal” in international policing. Presentation during the Third Challenge Training School on
The chapter has mapped the most important actors of the European intelligence community: national intelligence services, European institutions such as the Council and the Counter-Terrorism Working Group, and European information agencies such as the EUSC and INTDIV. In terms of counter-terrorism policy, the most important European information agencies are Europol and SitCen.

Most of the intelligence cooperation within the EU takes place bilaterally. Besides default sharing relationships between national intelligence services of EU Member States, this chapter has introduced some non-institutionalized sharing and discussion fora where Member States get together and discuss operational matters and trends, such as the Club of Berne.

The most important counter-terrorism EU decision makers in need of intelligence support are the Council and the High Representative. These actors should be supported with intelligence which satisfies a host of demands and requirements:

- The intelligence should be high-quality, and combine the best intelligence that Member States and European actors have to offer
- The intelligence should be both strategic and operational in nature
- A substantial amount of intelligence should be sourced from OSINT
- The intelligence should be timely delivered to the right decision maker
- The intelligence should pass through a secure communication system that has options for compartmentalization
- The intelligence should contain a relevant amount of early warning and trend identification
- The use of intelligence should not infringe fundamental freedoms and/or human rights

The Office of the Counter-Terrorism Coordinator, located within the General Secretariat of the Council, is currently undergoing changes. The present Coordinator Gijs de Vries has left Brussels in May 2007, and a decision about the future has not yet been taken. In any case, the likelihood of the Coordinator actually being capable of coordinating Member State or EU policy remains slim. A successor to Gijs de Vries will most likely work with a different job description. The general ability of the EU to influence and coordinate...
national counter-terrorism policy remains limited, since counter-terrorism is and will for the foreseeable future remain a policy field firmly in the hands of the Member States.

Both Europol and SitCen are being called the leading EU agency in the field of counter-terrorism. Indeed, the delineation of tasks between the two bodies took some time to fall into place. SitCen is an intelligence service and provides support to the Second Pillar, whereas Europol is a police organization and provides intelligence support to the Third Pillar. An even greater synergy between the two information agencies is desired in the future, to continue to provide EU decision makers with high-quality counter-terrorism intelligence support. A good balance between security intelligence and police information should be struck.

Some national intelligence services remain skeptical about the EU’s role in counter-terrorism, and especially the intelligence support for this role. They argue that the strongest EU intelligence assets lie in the national intelligence services, and the EU should contain itself to facilitating their work.\textsuperscript{114} Europol’s

\textsuperscript{114} Interview with IISS Officer 2, 10 May 2007, International Institute for Strategic Studies Headquarters, London, UK.
and SitCen’s work do sometimes provide added intelligence value to the work of national intelligence services. However, national intelligence services are critical about the future expanding role of Europol and SitCen alike.

The full implications of both the Prüm Treaty and the principle of availability are not yet known to the European intelligence community. Direct access as a principle still seems a distant reality – yet if Member States take the principle of availability seriously this could go a long way in improving counter-terrorism intelligence sharing.
Chapter 5

General Problems in Intelligence Cooperation

5.1 Introduction

This chapter presents the findings of this study: the general problems in international intelligence cooperation, and specifically in counter-terrorism intelligence cooperation in the EU. The findings of this chapter are based on the literature review, the desktop findings and most importantly, the interviews conducted for this study.

This study’s research question is what are the most important problems in counter-terrorism intelligence sharing within the European Union, and how can these problems be resolved? This section aims to map the most important problems in improving counter-terrorism intelligence sharing in the EU. Interviewees have mentioned several problems that are obstructing European intelligence cooperation, which were not mentioned in chapter 1. However, the fact that these factors were brought up during the interviews, means that they constitute problems in the daily reality of the persons who are exchanging the intelligence. Some of the mentioned problems overlap with the problems mentioned in chapter 1 but they deserve some more attention under this section nevertheless. The problems are listed under their character: political, cultural, legal, organizational and technical.

5.2 Improved intelligence cooperation in the EU

It has been argued that terrorism is a severe threat to the European Union and its area of justice, liberty and security for European citizens. Furthermore, it has been established that intelligence and more specifically, intelligence
cooperation is one of the most important weapons at the European level to effectively fight this threat. Intelligence is central to the EU’s concept of intelligence-led law enforcement. Thus, improved intelligence cooperation is necessary to fight terrorism more effectively. The improved intelligence products that would result from such improved cooperation could provide more effective intelligence support to European decision makers, such as the High Representative. Furthermore, improved EU counter-terrorism intelligence cooperation would provide Member States with an incentive to continue to submit their intelligence to the European level.

As the threat of terrorism continues to grow more international (both in terms of networks and in terms of effects and consequences), it becomes too large for any single EU Member States to tackle alone. Member States need to cooperate (bilaterally, multilaterally, and on the EU level) to make complete and accurate threat assessments in the field of terrorism. Intelligence cooperation and improved information sharing is essential in this field. It can be impossible for a single agency or Member State to map the activities of an actor and to apprehend the magnitude of the threat, if the agency or Member State only takes into account those actions that fall under its specific geographical and functional responsibility.¹

The international threat of terrorism thus requires a collective European response. European and national decision makers have to coordinate and interlink the different security policy instruments at their disposal. Efforts of different countries and organizations have to be synchronized, in order to arrive at efficient policy and in order not to waste resources. Cross-border and cross-agency intelligence cooperation is vital in this context.²

Advantages of improved European intelligence cooperation

Improved intelligence cooperation within the EU would yield numerous advantages. Most importantly, the EU needs qualitative intelligence support for its policies in the field of security, defense, and foreign policy. Faced with a combination between ‘old’ and ‘new’ threats, the EU needs better intelligence

¹ Müller-Wille, B. (2003) SSR and European Intelligence Cooperation Implications of the New Security Challenges and Enlargement (Both EU and NATO) for Structuring European Intelligence Cooperation, as an Important Aspect of SSR. Conference paper for the 6th Annual Conference of the PfP Consortium for Defense Academies and Security Studies Institutes, Geneva Centre for the Democratic Control of Armed Forces. p. 3.

² Ibid.
support than it is receiving in this moment for many of its tasks, such as military operations, crisis management operations, and the St. Petersburg tasks. The existing EU intelligence function, as compromised of the European intelligence community, does not currently deliver the intelligence support needed. Promising steps have been taken but substantial developments are needed to ensure that the EU continues to provide security, freedom and justice to European citizens. The Union must be given the intelligence support it needs, if Europe is to produce security collectively throughout and within the EU.

Furthermore, increased intelligence cooperation would decrease dependency on US intelligence during crisis management operations in the Second Pillar. The dependency on US intelligence during the Gulf Wars and in Bosnia has been considered a weakness in EU intelligence policy, which some Member States were especially keen to solve. The most recent trans-Atlantic crisis over the fraudulent intelligence that lead to the invasion of Iraq for its alleged possession of weapons of mass destruction increased the desire of the EU to be independent of US intelligence for its decision-making in the Common Foreign and Security policy (Second Pillar).

The last important advantage of improved European intelligence cooperation would be that the EU would be able to provide real added intelligence value to the Member States. With added value provided by the EU, Member States will be motivated to continue to submit and share intelligence to and at the European level. Thus, improved European intelligence cooperation would be a positive self-fulfilling prophecy.

EU counter-terrorism and intelligence

In the Third Pillar of Police and Judicial Cooperation on Criminal Matters, the EU is implementing intelligence-led law enforcement. This is a method of preventing and combating all forms of crime, including terrorism, through

---

more efficient and effective use of available intelligence, for instance coming from community policing. Improved intelligence cooperation in the EU to fight terrorism is crucial in intelligence-led law enforcement.

Improved intelligence cooperation would allow better detectability of threats. New threats such as the ‘new’ terrorism are more difficult to detect than traditional ones. Terrorist threats especially may not become visible until they materialize, by which time it is too late. Improving detectability will require a development of collection methods and capabilities. This necessitates an intensified cooperation and exchange of experiences among various intelligence agencies.6

This study has given substantial attention to OSINT and the use of OSINT by national intelligence services and European information agencies. It has argued that OSINT deserves more policy attention than it is currently given, both at the national and at the European level.

Intelligence services are under increasing pressure from civil society and the media to prevent and thwart terrorist attacks. If an attack occurs, fingers are quickly pointed to the mishaps of national intelligence and/or security service. At the same time, societies are requesting ever more openness, transparency, and accountability from both national intelligence services and EU structures in the policy field.7

The exchanges and sharing of intelligence between national intelligence agencies, and all bilateral contacts that are related to these exchanges, have been and will always be an internal affair of the Member States. It may be suggested that the European Union continues to understand the crucial importance of bilateral exchanges for European intelligence cooperation. Without bilateral exchanges, there would be no European intelligence cooperation at all. Overall, these contacts manage themselves. The bilateral contacts need little stimulation from the European level to yield good results for all parties involved. It is recommended that the EU does not attempt to


replace bilateral contacts with multilateral contacts – intelligence cooperation between individual national agencies are the building blocks of the house of European intelligence cooperation.

In terms of national – European intelligence cooperation, the EU could take steps to stimulate and enforce this type of cooperation. Most of the exchange between national intelligence agencies and European information agencies is voluntary. Yet some (such as the sharing of criminal intelligence with Europol) could be better enforced at the European level. National – European intelligence cooperation is the next step after national – national cooperation, and it is time for the EU to take this step.

National – national information sharing is firmly in place. National – European information sharing still needs improvement, and European – European information sharing is an exception rather than a rule. The EU should occupy itself with stimulating national – European and European information sharing.

European – European information sharing is increasing. However, it is not yet at the level where it can provide real added value to European counter-terrorism policy. Once Europol is firmly established as the European criminal intelligence agency, and SitCen has been significantly increased in capacity and capabilities, better European – European information sharing in counter-terrorism is likely to be the (desirable) result.

EU Intelligence Support

No EU Member State has the means to equip itself at the national level with the whole array of intelligence gathering and processing components, which should provide an incentive for the Member States to use and develop the services of the EU information agencies. Ideally, the intelligence support function of the EU would originate from many sources. The information will mainly be supplied by intelligence and security services of Member States. But diplomats, local EU officials, Commission delegations, and Special Representatives will also regularly submit information or intelligence to the

---

EU intelligence function. It is suggested that the EU should make better use of its existing network. The Commission delegates (128 overseas in total) represent a significant source of OSINT, and can be put to much more use than is being done today.\(^9\) Heavier use of OSINT and community intelligence are recommended.

The Future of EU Counter-Terrorism Policy

The EU continues to develop and implement counter-terrorism policy. However, the responsibility for counter-terrorism policy lies firmly in the hands of the Member States. The EU attempts to coordinate, facilitate and provide added value, but performs some of those tasks more successfully than others.

Overall, the EU is moving in the right direction. In the Second Pillar, according to Duke,

\[t\]he EU Member States have established direct means for the sharing of intelligence assessment within the CFSP structures (mainly via the Policy Unit, the EUMS and SitCen); the arrangements for the handling and classification of intelligence have been developed; the EU has, through its [EUSC], exploited its commercial satellite imagery more effectively; and the High Representative is supported with a wide array of analysis to back up his diplomatic and peacekeeping roles.\(^10\)

However, both in the Second and the Third Pillar, intelligence support to EU decision makers remains insufficient.\(^11\) European intelligence abilities must develop further to support the EU’s role on the international stage in the Second Pillar and an area of freedom, security and justice for all European citizens in the Third Pillar.\(^12\)

Counter-terrorism policy is demanding the EU to perform tasks in an area where it has always been relatively weak. Facilitating national law enforcement, including national intelligence services, would require a system that emphasizes the EU’s strong points and improves its weaknesses. Most national intelligence services frown upon the institution building and legislation

---

9 \textit{ibid.}
10 \textit{ibid.}
flourish that the EU has so far exhibited in counter-terrorism policy.\textsuperscript{13} They argue that the EU should focus more on facilitating benchmarking between national intelligence services, and the setting of common standards to even further simplify and stimulate bilateral exchanges.

Unfortunately, one of the things that would stimulate intelligence cooperation in the EU in a very powerful way, would be a large contingency. The terrorist attacks in London and Madrid were the largest incentives for intelligence cooperation of the last years.\textsuperscript{14} But other developments also could help the EU move in the right direction. The slowly decreasing importance of sovereignty coupled with the increasing interest of Member States in sharing information, should automatically lead to improved intelligence cooperation.

### 5.3 Political problems

**Willingness to share information**

The problem most often mentioned by interviewees is the lack of willingness to share information by national intelligence and security services. The political will of Member States to share information at a European level is without doubt one of the largest problems facing intelligence cooperation in Europe today. Member States are hesitant to provide ‘hot’ intelligence to European information systems such as Europol, since intelligence lies at the core of national sovereignty.\textsuperscript{15}

The hesitancy to share intelligence with European information agencies can be attributed to a number of causal factors. However, when it comes down to a basic cost-benefit analysis of the intelligence services, the cause of the hesitancy is rather straightforward. Sharing bilaterally gives much better results than sharing multilaterally. National intelligence services continue to report better results from national – national sharing than from national – European sharing.

\textsuperscript{13} Interview with IISS Officer 2, 10 May 2007, International Institute for Strategic Studies Headquarters, London, UK.

\textsuperscript{14} Interview with Europol Officer 1. 27 February 2007. Europol Headquarters, The Hague.

\textsuperscript{15} Interview with IISS Officer 1, 11 May 2007, International Institute for Strategic Studies Headquarters, London, UK.
Most national intelligence services publicly support the idea of European information sharing – however, the actual exchange with European information agencies such as Europol comes about slowly. Bilateral information exchange between national intelligence services, on the other hand, is a daily occurrence for most intelligence services. This is caused by the fact that throughout the course of a regular bilateral intelligence exchange, the information position of all involved actors is improved. European information exchange, on the other hand, often improves the information position of only one partner in the exchange: the European information agency. Added intelligence value from European products for national intelligence services is an exception rather than a rule.

While Member States agree in principle that coordination at the EU level is desirable because of the cross-border nature of the terrorist threat, they are hesitant to give the Union the powers (such as investigation and prosecution) and the resources (such as intelligence officers and resources) it would need to be more effective.16 This shows the need for the EU to provide real added value to the Member States to continue to provide them with incentives to submit intelligence to the EU intelligence function.

National intelligence services report that the products originating from the European agencies are often of little value17: it often concerns information that they already possess. Thus, these products can only serve as a confirmation of existing information. Thus, the information exchange with other national intelligence services gives better results for an average national intelligence service than exchange with a European information agency.18 European counter-terrorism intelligence cooperation is also hampered by a lack of results for national intelligence services. If the EU does not manage to provide substantial added intelligence value to the information position of the national intelligence services of the Member States, they will have little incentive to submit intelligence products to the European level. Concluding, lack of willingness is caused by the fact that national – European sharing provides poorer results than national – national sharing.

17 Interview with AIVD officer, 23 February 2007, AIVD headquarters, Leidschendam-Voorburg, the Netherlands.
18 Exploitation Policy of the Dutch Military Intelligence and Security Service (MIVD). April 2006
Issues of competition also play a role. Some intelligence services compete with other security agencies within their own Member State. In some Member States, Europol is seen as competition for the national police force, and information is not exchanged for this reason.\textsuperscript{19}

The third party rule (no exchanged information can be shared with third parties without the explicit consent of the source) also hinders the likelihood and willingness of information sharing at the European level.\textsuperscript{20} Many national intelligence services use the third party rule as an argument not to share information at a European level. Often, intelligence is first shared with other national intelligence services. With some delay, a “cleaned” version of the same intelligence will be shared at the European level.\textsuperscript{21}

**Third Pillar decision making and instruments**

Decision making structures in the Third Pillar makes efficient policy more difficult. Third Pillar EU decisions still require unanimity, instead of qualified majority voting such as other EU policy areas. The European Commission adds that the decision making procedures in the Third Pillar obstruct the emergence of a strategic vision in European law enforcement.\textsuperscript{22}

Legal instruments are also often implemented slowly at the national level. An example of slow implementation was the appointment of national contact points when the Europol system was being implemented at the national level.\textsuperscript{23} It took much more time than expected and considerably slowed cooperation between Europol and some Member States.

Many interviewees commented on the sheer number of formal but non-binding cooperation arrangements for European police cooperation. Indeed, the great number of non-binding instruments and arrangements does not make it easy for an average police officer to know which way to turn for increased information sharing. This problem is also recognized at


\textsuperscript{20} Exploitation Policy of the Dutch Military Intelligence and Security Service (MIVD). April 2006

\textsuperscript{21} Ibid.


the level of the European Commission, who says that the non-binding nature of recommendations in the Third Pillar obstructs more efficient police and intelligence cooperation.24

An increasing amount of legislation, cooperation agreements and formal channels of information sharing also creates another risk factor. Police and intelligence officers are pragmatic practitioners. They are looking for results, and are less interested in what forms these results are delivered. Thus, if formal arrangements of sharing do not smoothly connect to the daily reality of their jobs, they will go around and outside these formal arrangements to achieve the results they desire. They prefer directly doing business with other police and intelligence officers without bureaucratic interference.25

Such sharing arrangements that are born out of operational needs instead of political pressure are also usually very effective. A good example is the Cross Channel Intelligence Conference, which is deemed a success by its participants. This arrangement of intelligence sharing was initiated and designed by practitioners, and was created because of an operational need. It has very little bureaucratic involvement, and fits smoothly into the daily job of the practitioners.26 Such bilateral or multilateral police cooperation arrangements exist in many parts of the world, and are often preferred by practitioners over ‘politically designed’ sharing arrangements.27

24 Ibid.
26 Ibid.
5.4 Cultural problems

The absence of a culture of trust

Closely related to the lack of willingness to share information, is the absence of a culture of trust. The European Commission mentions the “building [of] trust between the relevant services” as a key factor in improving intelligence cooperation.\(^{28}\) This is due to the “lack of […] culture of cooperation between the relevant authorities and between public- and private-sector players.” The aim of the Commission is to “develop working relations between the Member States” with its information policy.\(^{29}\) The European Commission calls the lack of willingness of share information between law enforcement and intelligence agencies “understandable”. It hopes to build “a culture of trust and cooperation”.\(^{30}\) However, also the European Commission has not shown a consistent and clear vision on how to build this culture of trust and cooperation. It seems essential to invest in informal contacts and personal relationships between intelligence and police officers. However, to this day no concrete steps in this direction have been taken.

Linguistic and cultural problems also fall under the heading of absence of a culture of trust. Officers speaking the same language work together better than officers speaking different languages. However, in an EU of 23 languages\(^{31}\), linguistic problems are a rule rather than an exception. The building of trust is more difficult if a language barrier is in place. The same applies to cultural problems. Building confidence and trust is easier between two officers of the same or similar cultures.\(^{32}\)

Alexander Alvaro, Member of the European parliament, also stresses that there is no need for more legislation, but that a much more important goal is to bring people closer together.\(^{33}\) In other words, the European Union needs to

---


\(^{29}\) Ibid.

\(^{30}\) Ibid.

\(^{31}\) The official EU languages are: Bulgarian, Czech, Danish, German, Estonian, Greek, English, Spanish, French, Irish, Italian, Latvian, Lithuanian, Hungarian, Maltese, Dutch, Polish, Portuguese, Romanian, Slovak, Slovene, Finnish and Swedish.

\(^{32}\) The cultural problems will be more elaborately discussed in the next chapter.

\(^{33}\) Alvaro, Alexander (Member of the European Parliament, Committee for Civil Liberties, Justice and Home Affairs). Developing Europol Towards Efficiency and Accountability.
invest in soft measures to improve informal and personal contacts between police and intelligence officers. This, in turn, will automatically lead to better intelligence cooperation at the European and at the national level.

5.5 Organizational problems

The organizational diversity

Organizational diversity was also mentioned as a problem for initiating contacts. Some EU Member States have combined intelligence and security services; others keep them separate. Some have civil and military intelligence services combined in one single body; other Member States separate the two. Coordinating terrorism offices are getting increasingly common, but not all Member States have them. Police offices play different roles, in some Member States they are more active in counter-terrorism than in others. This results in problems with access to classified information: some bodies should have access to classified information from another Member State, some should not. Thus, the organizational diversity within Member States often poses problems for information cooperation.34

The European Commissions calls this problem the ‘compartmentalization’ of information, due to the fact that both at organizational and at a legal level, procedures on information exchange differ.35 The organizational diversity will continue to be a hampering factor for European intelligence cooperation, and its importance will grow with the accession of new Member States. Already, the ten Member States that acceded in May 200436 have different structures of intelligence and police than the older Member States. Quite often, the law enforcement structures of these new Member States are still based on old

Presentation during the Third Challenge Training School on Police and Judicial Cooperation in the Third Pillar of the European Union. 13 – 14 April, Brussels.
34 Interview with AIVD officer, 23 February 2007, AIVD headquarters, Leidschendam-Voorburg, the Netherlands.
36 The ten Member States that acceded to the EU in 2004 were Malta, Cyprus, Estonia, Latvia, Lithuania, Slovenia, Slovakia, the Czech Republic, Hungary, and Poland.
military structures, sometimes dating back to the Cold War. As the newer Member States enter into the European police cooperation agreements, the organizational diversity will continue to be problematic.\textsuperscript{37}

### No central inventory of counter-terrorism activities

Counter-terrorism policy at the EU level is a rather fragmented and non-transparent policy area. Many different bodies and working groups are concerned with counter-terrorism. However, there is no central inventory being maintained of what activity is being conducted and where. There is no dedicated body in Brussels that deals with all the aspects of counter-terrorism on a fulltime basis.\textsuperscript{38} All EU DGs are concerned with counter-terrorism, ranging from logistics to public health to trade. This can lead to duplication of activities at the national, and especially at the European level. A central, transparent inventory of EU counter-terrorism measures at the Commission level is seen as an important step forward by national intelligence services and many interviewees.\textsuperscript{39}

### 5.6 Legal problems

#### Legislation

Europol functions under strict data protection rules. It sometimes encounters legal problems when personal data needs to be stored for longer than 3 years. Data protection legislation is key to European intelligence cooperation because it intends to protect the privacy of European citizens, a fundamental freedom.\textsuperscript{40} Several Europol officers and national policemen reported some legal problems, mainly to do with data protection law, in storing information

---


\textsuperscript{39} Interview with AIVD officer, 23 February 2007, AIVD headquarters, Leidschendam-Voorburg, the Netherlands.

\textsuperscript{40} Charter of Fundamental Rights of the European Union, Chapter II Freedoms, article 8 protection of personal data. 18 December 2000.
in the Analytical Work Files. Individual officers fear legal proceedings against them personally if data is not exchanged in the correct manner causing problems in data exchange.\textsuperscript{41} Another legal problem exists in the differences between mandates in different Member States of the European Union. Intelligence collected in one Member State might be allowed as intelligence in a different Member States, which has a stricter mandate for its intelligence services. For instance, SIGINT collected in Poland might not be usable in Germany, where intelligence services function under a stricter mandate.

A balance needs to be found between the protecting of privacy of European citizens and the need for swift and easy exchange of intelligence to protect the security of European citizens.\textsuperscript{42}

### 5.7 Technical problems

#### The interoperability of databases

A large added value in European intelligence cooperation could be obtained by combining different intelligence databases. The opportunities that such combinations would yield involve comparing and adding data to different databases. For instance, Europol could be connected to the Schengen Information System II (SIS II).\textsuperscript{43} This principle is also known as ‘direct access’. Depending on the terms of implementation, the principle of availability could add substantial steps in this direction.

Many interviewees report problems with the interoperability of different databases because every national intelligence service and every national counter-terrorism body has a different way of indexing information.\textsuperscript{44} Furthermore, even communication systems between European institutions such as the Council, the Commission, and Europol are not connected.

\textsuperscript{41} Interview with Tayside Police Officer, Turin, Italy. 13 February 2007.
\textsuperscript{42} The balance between privacy, security, freedom, constitutional rights etc. will not be further discussed in this study.
\textsuperscript{43} Interview with Europol Officer 1. 27 February 2007. Europol Headquarters, The Hague.
\textsuperscript{44} Interview with AIVD officer, 23 February 2007, AIVD headquarters, Leidschendam-Voorburg, the Netherlands.
Therefore, exchanging information between databases or even connecting different databases leads to technical problems.\textsuperscript{45} This can be the case even within one Member State.

These problems can take many forms. For instance, the spelling of Arabic names is done differently in different Member States. Some Member States retain only the most basic information about terror suspects, such as names and dates of birth. Other Member States have more extensive information databases which leads to problems when Member States attempt to connect their respective databases.

The European Commission realizes these problems that are connected to the interoperability of databases. It stipulates that “compatible information exchange systems protected against unlawful access are [...] needed, as are common standards for information storage, analysis and exchange between the relevant services”.\textsuperscript{46} The European Commission says that “a number of databases and communication systems exist at European level. The main examples are: the EIS, the SIS, the CIS and the Customs Files Identification Database. There is a risk of duplication between some of them. The Commission also questions their interoperability. Three possible options should be considered: to merge the existing systems into a single “Union Information System”; to keep the systems independent and allow the creation of new systems as required; to investigate and implement the harmonization of the data formats and the respective access rules between the various systems.”.\textsuperscript{47}

Problems with data protection legislation are also almost unavoidable when connecting databases, as is discussed under the heading ‘data protection’, below.

**Secure means of communication – classification of information**

Some national intelligence services report a lack of secure means of communication to exchange information with European agencies such as the EU Council. Furthermore, there can be problems with the classification of


\textsuperscript{47} Ibid.
information: at the EU level, information might have a different classification code (e.g. Restricted, Confidential, Secret, Cosmic Top Secret) than at a national level. The European Commission indeed agrees that “common standards for information storage, analysis and exchange between the relevant services” are needed.
Focus: informal sharing and personal contacts

6.1 Introduction

A specific research focus was the use of informal arrangements and personal contacts in intelligence sharing. The absence of a culture of trust was one of the problems mentioned in the previous chapter. This chapter will discuss this specific problem more elaborately. The use of informal arrangements of sharing and the use of personal contacts while sharing will be discussed in this chapter.

Personal contacts are crucial in establishing and maintaining relationships of information sharing. Furthermore, personal contacts can increase the quality and quantity of shared intelligence. This chapter also introduces the concept of FORINT and the possibilities of this new intelligence approach for counter-terrorism intelligence cooperation in the European Union. Informal arrangements entail all non-formal arrangements of intelligence sharing that exist between intelligence officers and other practitioners. They can be bilateral or multilateral, but the majority of informal sharing within the EU takes place on a bilateral basis. Informal arrangements are often preferred over formal arrangements of sharing by practitioners because they are often more economical, pragmatic, cost-efficient, manageable and more integrated with daily operations than formal arrangements. The human aspect of intelligence sharing behavior will be more closely examined in this chapter.
6.2 Informal versus formal information sharing

In current arrangements of intelligence sharing in the EU, both formal and informal networks exist. Formal arrangements of intelligence sharing are formalized networks of information sharing, which have been agreed upon by policy makers, usually in the form of a Memorandum of Understanding (MoU) or other type of written agreement. They formalize practices and information exchange, and constitute attempts to move informal procedures to a controlled formal structure. Informal arrangements are the personal contacts that exist between personnel of police or intelligence services. They rely on a personal relationship built on trust and exchange intelligence through non-formal channels. No account is kept of which or how much information is exchanged. However, a fairly balanced relationship in exchanging information is crucial to maintaining this type of network.

The majority of intelligence sharing within the European Union is formalized. Exchange often goes through electronic channels, and in accordance with the designed procedures for information sharing. Informal sharing is explicitly discouraged. Intelligence services find it of the utmost importance to track which information exits. All information exchanges are recorded and processed. Intelligence services express a preference for so-called “one channel operations”, meaning that all information incoming and outgoing the service goes through a single channel.1

Informal arrangements

Informal networks exist independently of the formal arrangements of information sharing. Police officers and intelligence personnel do not easily relinquish the informal contact network that took years to build. Informal arrangements of exchanging intelligence also have many downsides. Services have little insight into which intelligence is exchanged and when. This way, the balanced relationship between intelligence services and the overall amount of intelligence exchanged can seem distorted. Intelligence services usually insist on monitoring exactly which and how much intelligence leaves the building.

1 Exploitation Policy of the Dutch Military Intelligence and Security Service (MIVD). April 2006
In practice, the EU Member States have a wide range of efficient, informal, bilateral (and sometimes multilateral) police cooperation and intelligence swapping structures. Of essential importance are senior police officers in the field of counter-terrorism that personally know many of their colleagues and – communicating by phone and email – form “efficient informal networks in and beyond the EU. Altogether these practices provide for swift and flexible responses and information exchange without the hindrances of centralized bureaucratic structures.”

Outside of the counter-terrorism policy field, informal networks of information sharing are seen as a valuable resource for organization. In disaster management, informal networks of sharing are used substantially more than formal networks. ‘Human bridges’ that can connect actors and organizations are needed in every organization and in every situation to ensure information flow.

**Formal arrangements**

Formal arrangements are institutionalized mechanisms of information sharing and have many advantages. Formal arrangements are designed to exchange information safely and timely. They give insights to policymakers into which information is shared, how often, and when. If formal arrangements are monitored properly, they can yield data about how to further improve information sharing.

An example of a formal arrangement for intelligence sharing is the so-called Prüm Convention. Signed on 27 May 2005 by Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Spain (and soon to be joined by Finland) it allows the law enforcement authorities of different countries to have direct online access to one another’s databases, compare DNA profiles and fingerprints, and exchange the corresponding personal data. The Schengen Information System SIS is another example of a formal arrangement of information sharing.

---

2 Block, L. European Counter-Terrorism Culture and Methodology, Terrorism Monitor, Volume 3, issue 8, 21-Apr-05.

3 Ibid.


However, formal arrangements often can be far removed from the daily realities of police officers and intelligence personnel, despite the fact that these arrangements are designed for efficiency and accountability. Police officers and intelligence personnel sometimes do not abandon the informal networks they might have been accustomed to. Moreover, these types of formal arrangements add to an increasingly unclear forest of communication channels that are available to law enforcement officers both at the national and at the EU level. 6

Research on police cooperation concludes that what is resisting the success of formal arrangements for intelligence sharing is the resistance from operative personnel, since these arrangements are not designed with their needs in mind, while they are the intended persons to do the actual sharing. Cooperation agreements and information exchange mechanisms never replace the informal networks that police officers have built over the years.7

What can be concluded from this is that it is not the organizations that matter in relationships of information sharing, but the officers actually doing the sharing. Personal relationships play an important role in sharing8. Informal manners of intelligence sharing are much preferred over formal arrangements, even within one organization.

Rational Choice

Research on police cooperation generates important results regarding the choice of individual police or intelligence officers to choose a formal versus an informal channel of sharing. Den Boer and Spapens argue that the choice is made pragmatically: it depends on where facilities, expertise and other resources are available. The same term –pragmatic- is used by a former intelligence officer who was interviewed for this study. Sharing relationships are pragmatic: this means that if an arrangement proves to be cumbersome (for instance due to complicated legislation), officers will find a way to work around it.9 If such resources are accessed most optimally through formal channels, law

7 Ibid.
8 Interview with IISS Officer 2, 10 May 2007, International Institute for Strategic Studies Headquarters, London, UK.
9 Interview with IISS Officer 2, 10 May 2007, International Institute for Strategic Studies Headquarters, London, UK.
enforcement officers will prefer formal channels. If however, their prediction is that better results will be achieved through informal channels, they are likely to make a rational choice for the latter.

Rational choice theory\(^\text{10}\) can be used to explain the behavior of intelligence officers when exchanging intelligence. They act in self-interest when they decide about whether or not to share intelligence and with whom. These interests could be varied and go both in favor or against intelligence sharing. When deciding whether or not to share intelligence, the following non-exhaustive list of interests could be applicable:

<table>
<thead>
<tr>
<th>Reasons not to share</th>
<th>Reasons to share</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ They have a natural tendency not to share intelligence</td>
<td>■ They are interested in sharing in order to improve their information position</td>
</tr>
<tr>
<td>■ They fear legal proceedings for violating data protection law if they share informally</td>
<td>■ They fear losing their job if they do not share because they have been instructed to share</td>
</tr>
<tr>
<td>■ They fear the compromising of their sources if they share intelligence</td>
<td>■ They feel obliged to share because of political pressure</td>
</tr>
<tr>
<td>■ They have concerns about a secure method of communication for sharing</td>
<td>■ They share to help out a friend or acquaintance with a different intelligence service</td>
</tr>
<tr>
<td>■ They fear that the receiving party will not handle their intelligence with the correct level of confidentiality</td>
<td>■ They try to comply with European legislation</td>
</tr>
<tr>
<td>■ They do not want to share information that gives them a relative advantage over a different intelligence service within their own Member State, e.g. a rivaling or sister organization</td>
<td>■ They try to comply with national legislation</td>
</tr>
</tbody>
</table>

\(^{10}\) Rational choice theory was elaborated on in chapter 1. It assumes that each action has a known outcome, and individuals can choose with capacity, time, and emotional detachment about the course which is most in his or her self-interest by weighing costs and benefits, risks and rewards.
When deciding between a formal and an informal arrangement of information sharing, the following non-exhaustive list of interests could be applicable:

- They will prefer using arrangements that have been used before
- They will prefer the arrangement that best fits their daily mode of operations
- They will prefer the arrangement that is most time-efficient
- They will prefer the arrangement that is most cost-efficient
- They will prefer the arrangement that delivers the best results
- They will prefer to share with persons they know personally, friends and acquaintances
- They will prefer the arrangement that best fits the particular exchange at hand
- They will prefer an arrangement in a language that they know and understand
- They will prefer an arrangement which cultural properties are similar to their own

In any case, individual intelligence officers are likely to obey the rules of intelligence mentioned in chapter 1. A rather strict balance in quantity and quality of shared intelligence products will be maintained between different intelligence services (quid-pro-quo) and intelligence will not be shared with third parties (the no third party-rule).

**Economical and pragmatic decisions**

Police and intelligence officers will design their informal arrangements of sharing, if formal arrangements are not available, sufficient or convenient to use. Examples of such pragmatic cooperation are Nebedeag-Pol (a joint commissariat between The Netherlands, Belgium, Denmark and Germany), and other regional arrangements in European border regions. The Euroregional Police Information and Coordination Center (EPICC) was established as a result of practitioners’ initiative. In this center, sixteen police officers and civil servants from public prosecutors from three countries cooperate and exchange information.11

---

Informal arrangements will spring up if formal arrangements are deemed insufficient. Law enforcement officers, when confronted with a constant gap between their needs and the ‘chaotic’ reality of EU institutions, prefer to create facts on the ground, ahead of political initiatives and arrangements. Furthermore, the existing arrangements do not always correspond well with the day-to-day operations of a law enforcement practitioner, leading him/her to prefer informal, tailor-made arrangements of information sharing.

Indeed, many interviewees commented on the patchwork of formal arrangements available at the EU level. Many different arrangements for information exchange already exist, and many new ones have been added at the EU level in recent years in response to terrorist attacks on European soil, amongst others. Examples are Interpol, Europol, SIS, joint commissariats, liaison officers, informal contacts, and (future) direct access to other databases. Law enforcement officers referred to the chaotic nature, the number and overall complexity of this jungle of existing arrangements as problematic.

Often, law enforcement practitioners prefer informal arrangements of sharing over formal arrangements. As has been explained, this is caused by the fact that informal sharing is often faster and yields better overall results. Block describes an increased demand for vertical law enforcement cooperation and the same can be said about a trend towards informal sharing.

**Vertical and Horizontal Cooperation**

Especially within literature on international police cooperation, the difference between horizontal and vertical forms of cooperation plays a prominent role. This section aims to clarify the differences between the horizontal-vertical division and the formal-informal division used throughout this study. It must be noted in passing that many similarities exist.

---

13 *Ibid*.
14 *Ibid*. 

Vertical cooperation can be compared with formal arrangements of sharing. Indeed, vertical cooperation is often characterized by formal structures. It usually takes the shape of traditional hierarchical cooperation, such as through the National Bureaus of the Interpol system.

Horizontal cooperation, on the other hand, is more similar to the concept of informal sharing used in this study. Competent organizational components cooperate at a similar level in a different Member State, even going down to individual law enforcement officers. The cooperation is decentralized, and solutions created by these types of cooperation can be tailor-made to a local problem.\(^{15}\)

The difference between horizontal-vertical and formal-informal divisions thus lie in different points. Firstly, horizontal-vertical points towards a hierarchical relationship, whereas formal-informal indicates the manner of communication in a cooperative relationship. Secondly, informal contacts need not be decentralized: also central organizational components can exchange information in an informal manner. Thirdly, vertical cooperation usually concerns topics such as EU-wide solutions, and high profile targets. Horizontal cooperation usually focuses on regional security cooperation, and solving day-to-day problems. Within the formal-informal division, no such restriction on topics exist. Information on any topic can be exchanged through formal channels, and this is even more so in the case of informal sharing.

### 6.3 Foreign Intelligence (FORINT)

#### Introduction

This section aims to introduce the concept of foreign intelligence, or FORINT. Foreign intelligence in this section refers to intelligence acquired through international intelligence cooperation. In other studies, foreign intelligence is understood as intelligence about other countries, literally ‘foreign intelligence’. However, when referring to this concept, this study uses the term “external intelligence”, such as the mandate of SitCen. In this study, foreign intelligence will therefore refer to intelligence acquired through cooperation with other
Focus: informal sharing and personal contacts

national intelligence services. FORINT is elaborated on in this chapter, under the heading of informal arrangements of sharing and the use of personal contacts, since personal contacts play such an important role in FORINT.

Based on an Israeli initiative, many European intelligence services are also realizing that intelligence exchange is underutilized as a means of acquiring new information. The Israelis were the first to announce that the acquisition of intelligence through other intelligence services would be as important as the acquisition of intelligence through SIGINT or HUMINT. They call intelligence acquired from other intelligence services “foreign intelligence”, or FORINT. They have announced investments in resources and personnel to make FORINT as important as HUMINT and SIGINT.

FORINT represents an important step forward in the use of intelligence to combat terrorism due to its promising results in stimulating intelligence cooperation. Terrorism can only be efficiently combatted if EU Member States work together, especially in the field of intelligence. The concept that FORINT is as important as SIGINT and HUMINT helps towards the goal of better and more efficient intelligence exchange within the EU. FORINT acknowledges the importance of the people exchanging the intelligence and emphasizes personal relationships over procedures and organizations. In short, people matter in FORINT.

This difference in personnel appointments has immediate effect on the information flow into and outgoing from the Israeli intelligence services. They are the initiators of this FORINT movement, which is attracting an increasing large following, also within Europe.

The FORINT sequence

The first step of the FORINT approach is a clear idea of the needs of other intelligence services. Israeli intelligence services employ analysts to paint a clear picture of what information all European intelligence services are desiring. For instance, Israeli intelligence services find out that German intelligence services are interested in the internal security situation in Somalia. This marks the beginning of the second step in the FORINT process: the unrequested sending of products. Once the information desires of a certain national intelligence service have been mapped, the Israeli intelligence services start feeding products on this topic without being requested to do so. Usually this concerns products that are of little importance to Israeli intelligence services. However, these products can be very valuable for the recipient of the information.

This has two consequences. Firstly, the information position of the recipient of the information on the desired topic is improved. And secondly, the strict adherence to the quid-pro-quo principle causes the recipient of the information to be more likely to send products to Israeli intelligence services. This increases the flow of information between the two intelligence services.

Furthermore, FORINT is characterized by a strong emphasis on the human factor of intelligence sharing. FORINT dictates that personal contacts and informal channels of information sharing are important. Therefore, FORINT targets people within organizations, instead of functions, in order to establish contacts of intelligence cooperation. The emphasis on the human factor is another reason why FORINT is such a successful method for increasing and improving intelligence cooperation.17

The emphasis on an overview of which products leave or enter a national intelligence service can hardly be overstated. If relationships of intelligence sharing are based on personal contacts rather than formalized channels (which is partially the case in the literal application of the FORINT idea), an

Focus: informal sharing and personal contacts

intelligence service can easily lose track of which products are shared.\textsuperscript{18} The promising concept of FORINT is opposed by some national intelligence services for exactly this reason.

Bilateral intelligence sharing arrangements can also be established without personal contacts. Usually, in this form of cooperation, two national intelligence services agree on a MoU or other formalized cooperation agreement. However, this type of cooperation is unlikely to substantially improve the information position of either of the partners of the agreement. When the sending partner does not trust the receiving partner completely with his intelligence product, usually only old or OSINT products will be shared. Only after a form of personal contact has been established, does the relationship gradually improve. Once the sending partner trusts the ability of the receiving partner to keep their products confidential, whilst also taking into account the other important rules governing intelligence cooperation\textsuperscript{19}, a process of confidence building can begin.\textsuperscript{20}

The importance of personal contacts does not finish there. Visits and face to face meetings at events, such as conferences, maintains and reinforces the established relationship between the persons sharing. During conference breaks, informal sessions and dinners, the details of intelligence cooperation are discussed and confirmed. A majority of the successes of bilateral international cooperation can be attributed to such informal encounters.

Thus, the preferred method of international intelligence cooperation for most intelligence officers consists of a combination between formal and informal arrangements. The formal arrangements are used to initiate contacts, which usually occurs on director or vice-director level. The formal arrangements also provide the necessary hard- and soft-ware, such as secured connections which are used to exchange intelligence products. However, the real successes of the cooperation depend on informal arrangement. A friendly and personal relationship with the cooperation partner ensures the results: receiving of good and valuable intelligence products. Regular informal

\textsuperscript{18} Interview with Officer of the Intelligence Division (INTDIV) of the European Union Military Staff. EU Military Staff Headquarters, Brussels. 12 April 2007.

\textsuperscript{19} Most notably, the quid-pro-quo principle and the third party principle. These unwritten rules governing international intelligence cooperation have been discussed in chapter 3.

\textsuperscript{20} Interview with Officer of the Intelligence Division (INTDIV) of the European Union Military Staff. EU Military Staff Headquarters, Brussels. 12 April 2007.
meetings and other forms of contact (through email and telephone) ensure the continuation of the personal relationship, so crucial to the success of intelligence cooperation.21

### 6.4 The human factor

As was explained in the introduction of this chapter, intelligence cooperation is heavily influenced by human behavior. Information sharing procedures are designed to facilitate intelligence cooperation between organizations; however, in the end it is always a person who has to make the decision to exchange an intelligence product with another person. Therefore, a certain human factor plays a significant role in every intelligence exchange. The following section will discuss some of the possible problems individual intelligence officers tasked with international cooperation could encounter.

#### Preferences of operational personnel

In the intelligence and security field, many formal arrangements for intelligence sharing exist. These initiatives, treaties and mechanisms are however characterized by their complexity and overlapping competencies. Especially amongst police officers and intelligence personnel, cooperation agreements are considered complicated, time consuming, and rather ineffective, especially when compared to informal procedures and personal contacts. Moreover, the design of formal arrangements for intelligence sharing rarely takes into account how new rules and regulations might or might not fit into existing structures. Most intelligence personnel express a strong preference for personal exchange between trusted colleagues, i.e. informal arrangements, instead of the sharing of intelligence through formal procedures for these reasons.22

In Alain’s research on police cooperation between Belgium and France, it transpires that formal requests for information sharing are seen as a last resort for police officers. Only when they are sure that the desired information is available in no other way than an official request, will they use formal

---

21 Ibid.
Focus: informal sharing and personal contacts

arrangements of intelligence exchange. This following quote shows that informal arrangements of information sharing are strongly preferred over formal structures and procedures: “First of all, I’ll contact someone I know from this or that country. When I know that the information I seek is available, then only I’ll think about engaging the formal procedure.” 23 Other research papers on police cooperation shows that practitioners like to contact people who are similar to themselves: closer geographically, or officers with whom they share a resemblance. 24 Similar results have been found by other researchers in the field. For instance, a study on Europol and terrorism emphasized that “an average Dutch police officer is more likely to call a befriended officer in Milan to inquire about an Italian criminal than to call Europol in The Hague.” 25

Various interviewees stressed the importance of personal contacts when relationships of intelligence sharing are being maintained. “If you know each other, everything is just that much simpler. It makes the difference between a formal cooperation based on MoU’s and yielding few results and cooperation between friends, yielding excellent results.” 26

The preferences of operational personnel have been described in literature on law enforcement cooperation and many interviewees of this study. Direct informal police cooperation between individual officers was and still is a widespread practice in Europe. 27 The information age has only led to an increase in informal personal contacts between law enforcement officers all over Europe. European law enforcement cooperation “is already a reality in the address books of police officers”. 28

26 Interview with Officer of the Intelligence Division (INTDIV) of the European Union Military Staff. EU Military Staff Headquarters, Brussels. 12 April 2007.
Chapter 6

Resources

The first and most important factor influencing the behavior of intelligence officers is the availability of resources. Intelligence officers usually have a lot on their plate: an extra task - especially if it concerns a task that is believed to be relatively useless - is seen as an unnecessary burden, and the intelligence officer is not likely to spend much time or effort on it. The task of international intelligence cooperation will take time away from daily tasks and responsibilities. Intelligence officers might not be motivated: they might experience little support; they might be unfamiliar with the topic of intelligence cooperation; they might experience language problems. The results from international intelligence cooperation are often less useful than results from bilateral intelligence exchanges. Thus, not only are fewer resources available for international information sharing, it also receives a lower priority than bilateral information sharing because of its likelihood of yielding poor results.

Personal Relationships

Once a personal relationship is established between intelligence officers or practitioners, it is much easier to start a relationship of information sharing. Some interviewees even go so far as to say that it is virtually impossible to start an information exchange, without personally knowing the person who is on the other side of the exchange. One interviewee talks about the importance of personal contacts within information exchange:

*This analyst is a friend of mine. I know him, because we used to work together in [country of origin]. We talk professionally, but also on a [...] more personal level. It’s just developed really well over the last few years. So we are in contact almost daily – and the information flow back and forth is substantial, if you know what I mean. He sends me something, and I send something back.*

The language barrier also plays a role here: best results are achieved mostly in bilaterals in which the partners speak the same language. Sharing is possible also without such a personal relationship; however, practitioners estimate the chances of results of such sharing as substantially lower.

Once a relationship of information sharing is established, the actual information exchange often runs through formal channels. An example of this is Europol, which maintains a secured formal network to exchange information with the Member States. All Member States are connected to this network; they can request information, and send each other messages over this secure connection.

The importance of personal relationships between law enforcement officers for initiating an intelligence exchange has been discussed in this chapter. Furthermore, various interviewees have stressed that human factors are always more problematic than legal or technical barriers. The human factor works at the local, national and international level. The human factor also plays a role in the results of cooperation. If personal contacts are established within a team composed of different players, such as a Europol Joint Investigation Team, results are usually much better. Not surprisingly, Joint Investigation Teams only consisting of two Member States and Europol (bilateral) yield the best results. As a general rule, the fewer players a team has, the better the results are likely to be.

The personal relationship between police and/or intelligence officers forms the basis of a relationship of information sharing. A relationship of information sharing can be described by the following steps, showing that confidence is at the basis of such relationships.

---

Confidence is thus needed before any communication of intelligence cooperation can take place. When a step (e.g., from communication to coordination) is taken successfully and the confidence basis is intact, the relationship can take a step to the next level. The last level is coordination, whereby two officers from different intelligence services coordinate their investigations, ensuring that no overlap exists and attempting to create synergy between the two intelligence services.

Opinions on intelligence cooperation

Throughout this study, the idea that intelligence cooperation is in essence beneficial for both parties is supported. It has been argued that no effective EU counter-terrorism policy can exist without intense and substantial intelligence cooperation at the national and the EU level. Most interviewees, especially at the European level, agree with this statement and support it in practice. Most interviewees stress that intelligence cooperation is a necessary part of their job.

However, some interviewees (especially intelligence officers from national intelligence and security services) point out that sometimes European intelligence cooperation is “forced” upon them by politicians, both at the national and the European level. National exploitation policies of intelligence services mention that little attention is paid to contacts that are forced upon them by politics. These contacts prove of little or no value to national intelligence services in their perception. Thus, national intelligence services are hesitant to commit time and resources to international cooperation that is “forced” upon them, rather than initiated by themselves to improve their information position. They argue that intelligence cooperation is not always necessary, and that European intelligence cooperation in general gives them poor results. However, if politicians force intelligence services to cooperate at the international level, individual officers are tasked with this cooperation. In this case, intelligence exchange is likely to be slow and problematic: since no sincere desire exists to cooperate, any cooperation will be seen as a burden rather than an advantage.

Furthermore, the culture of some national intelligence services can be characterized as “skeptical.” The expectations on results of intelligence cooperation are low. Furthermore, rivalry might exist between agencies within the same country about who is tasked with international cooperation. Other
problems include: logistics, communication, the incompatibility of timescales, or so-called NIMBY-ism: Not-In-My-Backyard. This term refers to the behavior of intelligence officers when they agree to a certain amount of cooperation, but refuse to commit time or other resources from their own organization. 35

**Language and culture**

The importance of the language barrier in the European Union, which hosts an impressive 23 official languages, is often underestimated in studies of different kinds of European cooperation. The results of cooperation between partners is often much better when they speak the same language, or are relatively proficient in a common language. Despite the fact that seconded police and intelligence officers usually speak and understand English, this does not take into account that second-language communication is usually much less effective than first-language communication.

Some interviewees have stressed the importance of language courses for those police and intelligence officers who are responsible for intelligence cooperation. The funding of language courses for officers tasked with international cooperation is an excellent example of a ‘soft measure’, which could be taken to improve European intelligence cooperation.

A similar argument could be made about national cultures, and their effects on cooperation at the European level. Some EU Member States have long-running histories with terrorist attacks, such as Spain and the UK. Consequently, they have a different sharing culture than Member States who have fewer experiences with terrorist attacks. Yet culture also plays another role in processes of cooperation. If a team is comprised of nationals from different Member States, and from different cultures, the effort required to achieve the same results as a mono-cultural team is much greater. 36

**Trust**

The important of trust in a relationship of information sharing can hardly be overstated. For this study, trust can be defined as the belief that the relationship will be mutually beneficial, that confidentiality will be maintained

---

and that the rules of intelligence sharing\textsuperscript{37} will be obeyed. Thus, the sending party expects something in return for a piece of information that is shared. At the same time, trust concerns the confidentiality of information. When information is exchanged, the sending party trusts the receiving party to keep the information confidential, and obey the “no-third-party” rule that is so essential in the intelligence community.

The fact that trust is a sine qua non for relationships of information sharing, has been stressed in the literature, at conferences, attended training schools and by virtually all interviewees for this research. ‘No exchanges take place without confidence and trust’\textsuperscript{38} seems to be the underlying assumption of police makers and practitioners involved with information sharing.

\section{Conclusion}

An efficient network of intelligence sharing already exists in the EU. A large majority of this information sharing takes place on bilateral basis. A small minority of the sharing takes place in a more international setting through an EU information agency such as Europol or SitCen. That being said, the importance of informal networks of sharing for the net amount of shared intelligence in the EU can hardly be overstated.

Unfortunately, national intelligence and security services have a negative attitude towards informal sharing. This is caused by the fact that with informal sharing, they cannot keep a complete overview of which intelligence is shared, and which intelligence is received. The so-called “one channel operations” principle stipulates that all shared and received intelligence should go through one channel. With informal sharing, this is hardly ever the case.

The use of personal contacts and informal arrangements diffuses the concept of single source communication. Individual intelligence officers exchanging products with other individuals in different agencies creates a chaos of sharing and receiving. The agency no longer knows which products have been sent and received, which is a situation they want to avoid at all costs. This fear is shared by intelligence agencies and police alike. In

\textsuperscript{37} See findings from literature study, chapter 1.
a situation where many organizational components (even in the form of individual officers) exchange and receive intelligence, it can become unclear which organizational components are in possession of which intelligence. Thus, informal sharing is actively discouraged by most national intelligence services.

Nevertheless, informal sharing remains an intrinsic element of European intelligence cooperation. Personal contacts are often necessary to initiate a relationship of information sharing. After the initial contacts, they are used to improve the quality and quantity of shared information. If an intelligence officers needs to share a piece of intelligence, and no formal arrangement is available to do so, practitioners are known to create their own methods of sharing. These are often based on personal contacts and bypass administrative procedures. Informal sharing can be said to be the preferred way of sharing in the opinion of pragmatic practitioners who are looking for fast results.

The preferences of practitioners and operational personnel can be described as economic and pragmatic. Thus, they prefer the sharing arrangement which is most economical in terms of costs, time, and administrative procedure. A short procedure will be preferred over a long one; a cheap one over an expensive one; and an administratively simple one over a cumbersome one. In practice, this means that informal arrangements of information sharing will virtually always be preferred over formal arrangements by practitioners and operational personnel.

The concept of FORINT has been discussed in this chapter. A relatively new approach in the policy field of intelligence sharing, it is based on the importance of personal relationships and the importance of international cooperation for the position of a national intelligence service. The FORINT approach looks promising and holds much potential for stimulating counter-terrorism intelligence cooperation in the European Union.

Various factors play important roles in regulating the behavior of intelligence officers when sharing intelligence through international formal channels. Restraints of resources, language problems, the absence of trust, time constraints, and cultural differences contribute to making international intelligence cooperation more difficult than bilateral sharing.

---

Chapter 7

Recommendations

It has been established that the EU needs improved intelligence and information sharing, if it is to fulfill its goal of providing security to European citizens. This chapter will discuss some recommendations and suggestions to improve the intelligence support of EU information agencies, and to improve intelligence sharing within the EU. These recommendations are based on the findings from the literature review, the previous chapters, and the aforementioned problems that were mentioned by the interviewees of this research. The conclusions made throughout the study have formed the basis for these recommendations, but are not addressed individually.

Ideally, all intelligence flow between national intelligence services and EU information agencies, and between European information agencies themselves, will have to take place over secure networks. All formal arrangements of information sharing will connect smoothly to the daily operations of intelligence officers, and their number and complexity will be significantly reduced. EU decision makers realize that informal arrangements of information sharing do, and will continue to play an important role. EU decision makers are not afraid to invest and promote the use of these informal channels, while keeping close watch on accountability, data protection legislation and the fundamental freedoms of European citizens.

7.1 Political recommendations

Scope of intelligence

The EU needs to expand its scope of the understanding of counter-terrorism intelligence. As has been argued in chapter 2, developments in intelligence cause the scope of intelligence to be substantially wider than before. Open source information, COTS (commercial off the shelf) products, public databases, academic research, products from think tanks and research
institutes, information supplied by diplomats, military personnel, international students and frequent travelers are sources of information that were not previously regarded as intelligence, but that now constitute an invaluable source of it. The scope of intelligence needs to merge from military or civil to military-civil; from national or international to both; from state or terrorists to state-sponsored terrorism. The definitions of all relevant terms need to be expanded: security, terrorism and intelligence nowadays comprise much larger areas than before.

The targets have changed, along with the methods and the sources, so cooperation is more important than ever before. The amount of information available from both open and closed sources is simply too much for any single European Member State to process and analyse.

The concept of community intelligence should also be incorporated more in the EU and national counter-terrorism policy. Community intelligence refers to information that is picked up at the level of the community. It can refer to various types of information. For instance, the guard of a large apartment building notices suspicious activities in one of the flats. A traffic policeman stops a car with individuals who display suspicious behavior. Or a schoolteacher notices signs of radicalization in one of her students. This information can be crucial, when a possible case of terrorism is being investigated. However, currently neither the EU nor most national intelligence services make use of this type of information. As community intelligence will continue to show its value for sounds counter-terrorism policy, its role as a crucial intelligence source will have to be recognized at the national and the EU level.

It is recommended that the EU expands its scope and flexibility of intelligence to an increased number of non-traditional sources and methods to counter current threats to its area of justice, liberty and security. The concept of intelligence-led law enforcement should be engrained in the entire EU intelligence community.

**EU information agencies**

The EU information agencies should focus on delivering better results to national intelligence agencies. This will be the single most influential development which would greatly stimulate national – European sharing. If
EU information agencies can provide substantial added intelligence value to national intelligence services, intelligence cooperation will be greatly increased.

The performance of the EU’s external intelligence function, represented by SitCen, can be greatly improved by adding capacity and resources to SitCen. A considerable expansion of this center would allow better general situational assessments that are tailored both in terms of time and contents to the agenda of the Union and its diplomatic efforts. It would improve the ability to make assessments evaluating possible threats to EU field staff. The SitCen needs to be expanded and its system for tasking needs to be revised if it is to give the intelligence support needed for different EU security policy tools.¹

SitCen has a clear counter-terrorism mandate in the Second Pillar of Common Foreign and Security Policy. The other European information agency with a clear counter-terrorism mandate is Europol, who performs its tasks in the Third Pillar. A special section of this study was devoted to their seemingly overlapping mandates. As terrorism will continue to be a threat to the EU, the synergy and continued cooperation between these two bodies will have to be closely monitored.

Europol is working hard to gain the trust of Member States to become the European criminal intelligence body. Indeed, the relevance and importance of Europol has increased over the last few years. Europol can only provide added intelligence value to EU decision makers and Member States if it receives good and timely intelligence from national police forces. Several EU legal instruments have been passed to ensure this goal – however, not all of these instruments are strictly adhered to by Member States.

The incorporation of Europol into the EU’s institutional framework is a desirable development, given the concerns about the agency’s accountability. However, this must not interfere with Europol’s current task and workload. Given the probable effort that such an incorporation will surely entail, it is questionable whether the increased accountability will be worth such an effort.

The JITS (Joint Investigation Teams) that Europol takes part in have great potential for the combatting of transnational organized crime. Terrorism could also be the subject of a Joint Investigation Team. However, as with all Europol measures, the success of these teams depends on the amount and quality of intelligence it receives from the Member States.

Recommending measures to motivate Member States to submit more and better intelligence to Europol is not an easy task. Again, this comes down to the building of a culture of trust and the establishment of good personal contacts between national and Europol police officers. The success of Europol so far can largely be contributed to the network of liaison officers and national bureaus, and their personal contacts with national and Europol police officers. An increased use and growth of personal contacts could enhance cooperation of national police forces with Europol further.

Another manner in which a culture of trust could be established would be multiple positive experiences of a national police force with Europol. If Europol can prove their added value (e.g. through the successful conduction of an operation together, or the provision of an analysis which helps an investigation in a Member State), national police forces will be more likely to submit their intelligence about investigations to Europol in the future as well. Of course, the problem remains the initial contact and the first-time submission of intelligence. Again, this could be improved by further nurturing the personal contacts between national and Europol police officers.

The principle of availability should be a useful tool for Europol as well. As Member States are stimulated to share more intelligence amongst each other, Europol could provide a bird’s eye view to Member States from the European perspective. Much depends on the practical conditions under which the principle of availability will be implemented.

There is little doubt that Europol should not only act as an extra resource for national police forces. It plays an important role in the European intelligence community, and should provide intelligence support to EU decision makers, mostly in the Third Pillar. Naturally, decision making power in the Third Pillar at the European level will be limited, because national security is a national concern. However, Europol should not hesitate to continue to move forward to become the EU’s criminal intelligence agency.

In an ideal world of intelligence sharing, Europol would also act as a European clearing house of criminal intelligence. However, in reality, Europol’s coordinating and distributing role seems a long way off. Member States will
likely remain hesitant about Europol’s fulfilling of this role. In any case, Europol should continue to act as an important discussion forum, an extra resource for Member States, and a center of expertise.

A secure communication system between Europol and SitCen should also be established. These two agencies both have a counter-terrorism mandate, and their efficient and effective cooperation is essential to EU’s counter-terrorism on the fault line between the Second and the Third Pillar. The present system of exchanging documents via couriers remains cumbersome and slow.

It is recommended that the EU information agencies fulfill the intelligence function for EU decision makers, and need to be given sufficient resources to perform this role. It is recommended that the EU information agencies deliver better results for national intelligence agencies. Synergy and cooperation between the EU information agencies should be guaranteed. Trust and confidence in EU information agencies should be encouraged and stimulated, for instance through nourishing personal contacts and positive experiences with the agencies for national law enforcement bodies. The principle of availability should be implemented in a way that it can fulfill its promising role.

OSINT at European level

The aforementioned information revolution concerns primarily intelligence from open sources, or OSINT. The increasing possibilities of accessing databases, the published research products of universities and think tanks, and online forums and platforms yield an enormous amount of information. However, the European intelligence community does not yet appreciate the full value and potential of OSINT for their intelligence products.

The amount of OSINT is virtually endless. Therefore, every national intelligence service needs increasing resources to manage their need for OSINT as a source for intelligence products. Since OSINT is by definition unclassified, there could be some value in analyzing and reporting OSINT at a European level. This would mean that individual Member States would retain their collection capabilities for all other methods of collection (SIGINT, HUMINT, CLASSINT, IMINT, ELINT etc.), but that OSINT collection and analysis would take place at the European level. This could be a task for Europol, the
Joint Research Center (JRC) of the European Commission or a new entity at the European level. A European approach of OSINT would be accompanied by the general concern for the security of classified information, and could at the same time provide a deeper and more thorough analysis than is possible at the national level.  

OSINT is also increasingly valued by practitioners as an invaluable tool in their daily operations. Says one Navy Wing Commander about OSINT  

\[\text{[...]} \text{if OSINT is 85% accurate, on time, and I can share it, this is a lot more useful to me than a compendium of super-secret material that are too much, too late, and requires a safe and three security officers to move around the battlefield.}\]

The Commission on the Intelligence capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission) indeed recommended the establishment of an OSINT Center within the Central Intelligence Agency (CIA), to ensure that the intelligence community in the US maximizes the use of publicly available, foreign print, radio, television, and Internet news and information. Specifically, the “dissemination and use of validated open-source intelligence inherently enables information sharing as it is produced without the use of sensitive sources and methods”.  

A European OSINT Center would make available to national analysts the mass of OSINT that is available in the world today, as the Commission WMD expressed for the US intelligence community. Furthermore, the establishment of a European OSINT center would allow for an easier integration of contributions from the private sector, which will play an increasingly significant role in OSINT collection, analysis, and dissemination in the future.  

A European OSINT center would signify an important step to the value and integration of OSINT in the European intelligence community. Furthermore, improved EU-generated OSINT would work towards the stated goals of providing better intelligence support to EU decision makers in the Second and Third Pillar, and providing real added value to the Member States. Such a European

---

2 Interview with Officer of the Joint Situation Center. General Secretariat, Brussels, 16 April 2007.  
5 Ibid.
OSINT center would have to receive a green light from important sharing fora such as the Club of Berne. Yet the potential of OSINT deserves more attention from European institutions. The scope of this research does not allow for extensive development of the idea of central OSINT processing at the European level, but the concept could be the subject of further investigation. Worth mentioning is a recent initiative named Eurosint, created at the request of DG JLS and DG RELEX which gathers all industry actors in Europe dealing with OSINT. They are technology firms providing hard- and software for collection and analysis, and analyst firms offering value added intelligence.

It is recommended that the EU develops OSINT at the European level with enhanced vigor. OSINT’s increasing relevance to EU counter-terrorism policy should benefit from improved selection and analysis at the European level.

**Investments in informal channels**

The FORINT approach, but also “general good sense” of intelligence officers dictates that personal relationships matter in exchanging intelligence products. Intelligence officers are more likely to share products when they personally know the receiving party. Personal relationships are especially important when initiating relationships of sharing. This has been discussed in chapter 6 as well. Intelligence services are hesitant to invest in ‘soft’ measures like personal relationships. Most intelligence services would rather invest in a new secure communication system, a new satellite for more SIGINT or new agents for increased HUMINT collection. However, given the success of the FORINT approach, the net result of investing in ‘soft’ measures might be equal or even greater than the results of investing in ‘hard’ or traditional measures. The EU could set an example by being a frontrunner in these ‘soft’ investments.

Thus, investing in personal relationships between intelligence officers would be a way forward, both at the national and the EU level. Investments could take the form of training courses, language education or conferences. During these events, different intelligence officers would meet and get to

---

6 Interview with IISS Officer 2, 10 May 2007, International Institute for Strategic Studies Headquarters, London, UK.
know each other. Besides the substantive part of training or a conference, substantial amount of time should be set apart for ‘hallway gatherings’, in which personal relationships can be formed.

Other examples of ‘soft’ measures that could be stimulated by the EU are language courses, and frequent meetings through conferences and/or workshops so that intelligence practitioners can get to know each other personally. Another soft measure is a commitment of the EU to a new level of training, recruitment, education, and assignments of personnel between and within agencies to broaden and deepen the knowledge base.7

Although these measures might seem very indirect manners of intelligence stimulation, they will likely contribute substantially more to the stimulation of counter-terrorism intelligence cooperation in the EU than ‘hard’ measures such as new secure communication systems.

It is recommended that the EU invests heavily in ‘soft’ measures to stimulate intelligence cooperation. Such ‘soft’ measures can include languages courses, conferences and workshops to nourish personal contacts between intelligence officers, training, recruitment, education and increased mobility of intelligence officers.

Collection Capabilities

The European information agencies do and will continue to fulfill their central role in the European intelligence community. European information agencies should be provided with the resources they need to fulfill their role: provide intelligence support to European decision makers and provide added intelligence value for EU Member States. The EU information agencies should continue to grow to perform a full-fledged EU intelligence function. However, this study has explicitly denied the need for collection capabilities for European information agencies such as SitCen and Europol. Collection capabilities could refer in this context to the deployment of HUMINT agents by SitCen, or the gathering of military intelligence by the INTDIV.

Firstly, the EU information agencies do not need collection capabilities. The strongest assets of the European intelligence community are the national intelligence and security services. These national intelligence agencies are usually well-developed, have sufficient collection and analysis capabilities and are experienced in providing intelligence support to decision makers. The EU should focus on strengthening its best points: providing synergy to national intelligence products, instead of doubling collection capabilities by desiring to develop its own. The EU should use the collection capabilities of the national intelligence services. In the future, an arrangement could be envisaged whereby EU information agencies could task national intelligence services, but this seems a distant future.

Moreover, an EU desire to develop its own intelligence collection capabilities would likely stir great resistance from many EU Member States. Intelligence lies at the heart of state sovereignty, and control over national territory and what takes place intelligence-wise on EU territory remains the responsibility of individual EU Member States. Thus, the development of EU intelligence collection capabilities is not a desirable or realistic option. The EU information agencies should continue to profit optimally from national collection capabilities to perform a full-fledged EU intelligence function.

It is recommended that the EU intelligence community functions without the development of its own collection capabilities. Its current strong points should be emphasized, by increased national – European sharing. In the future, a scenario could be envisaged where EU information agencies such as Europol or SitCen can task national intelligence agencies with a certain collection task.

7.2 Cultural recommendations

FORINT

FORINT has been discussed in chapter 6 as an exciting new concept within the policy field of intelligence sharing. Although it is still relatively ‘under the radar’ of national and European information agencies, its results so far have been promising.
The national intelligence agencies in the Member States need to realize the importance of the FORINT concept. This relatively new approach constitutes, in the opinion of the author and many interviewees, the future of intelligence cooperation. An increased emphasis on the importance of international cooperation would lead to better intelligence support to both national and European decision makers.

Demonstrably, the Israeli FORINT approach has led to a significant increase in intelligence exchange between Israeli and national intelligence services. A similar approach adopted by national intelligence services and EU information agencies could greatly improve European intelligence sharing.

An increased use of FORINT in European intelligence cooperation would also mollify the difficulties posed by the organizational diversity, as discussed under the previous section. The organizational buildup of counter-terrorism ministries and agencies differs in every Member State. However, since FORINT targets individuals instead of organizational components, this could bypass some of the difficulties associated with organizational diversity.

Ideally, such a FORINT approach would start with products comprised of OSINT or a low classification level (such as confidential) to initiate a sharing relationship. The sharing of OSINT or confidential products does not entail a great amount of risk for the sending party of the exchange. This would ideally lead to a building of trust between the sending and the receiving party, about the quality, confidentiality and reliability of the sharing relationship. Gradually, products with a higher level of classification could be exchanged.

It is recommended that the FORINT approach is seriously researched and considered by the EU as a method of stimulating EU intelligence cooperation.

Specialization of National Intelligence Services

The information revolution has caused a significantly larger amount of information to be available within the EU. This is largely caused by the rise of the availability of documents on the Internet. However, also other developments, such as an increase in the transparency of government institutions, play a role. This information revolution is likely to continue, and even to increase, as new ways of information access continue to be developed.
It has already been stated that currently, more information is available within the EU to be analyzed and processed by one single Member State. Even larger Member States such as the UK and Germany cannot cover all ongoing developments. Cooperation is again crucial.

The results of cooperation are greater when national intelligence services specialize. This specialization can occur on sources or on topics. For instance, Member States who have traditionally been strong players in the SIGINT field, should be encouraged to specialize further in the SIGINT field. Retaining a small HUMINT department, which does not render large amounts of valuable information, would be unwise in terms of resources. Some Member States traditionally have specific interests. The former colonies of France in Africa, such as Algeria and Morocco, continue to be of interest to French intelligence services. If national intelligence services would specialize more, the overall results for the EU on an aggregate level would be better.

It has to be noted, however, that most national intelligence services are only willing to specialize to a certain extent. National intelligence services have a desire to remain “information-independent”: this means that they do not like to be dependent on cooperation to receive certain types of intelligence. Thus, an initiative from the EU to encourage specialization of intelligence services is likely to meet a fair amount of national resistance. However, specialization remains one of the best ways to keep in control of a rapidly expanding body of information for the EU and for individual Member States.

It is recommended that the EU stimulates national intelligence services to specialize, thereby emphasizing and enhancing their strong points. National intelligence services should – in the future - abandon their desire to remain “information-independent”.

### 7.3 Organizational recommendations

#### Inventory of EU counter-terrorism measures

The counter-terrorism policy of the EU is a rather diffuse policy field. Most DGs of the EU are involved in some part of counter-terrorism policy. On the one hand, this ensures the involvement of many actors and resources in this important policy field to ensure the security of European citizens. On the other hand, it
is easy to lose track of the different EU activities in the counter-terrorism field. National Member States and their intelligence services experience problems in targeting the right EU actor to support their activities.

A central inventory of all EU activities would improve the oversight of EU counter-terrorism policy. It would enable all actors (national Member States and their agencies, EU agencies, and third countries and partners) to have a real-time, accurate overview of EU counter-terrorism activities. It would make it easier to target the correct EU partner for cooperation in this field. Such a central inventory of EU counter-terrorism activities could, for instance, be maintained by the General Secretariat of the Council.

It is recommended that the EU maintains a central inventory of all counter-terrorism measures.

The Counter-terrorism Coordinator

At the moment of writing the future of the office of the counter-terrorism Coordinator is not clear. The first, unofficial feedback on the office of Gijs de Vries is that Member States will not allow the EU to fully coordinate their counter-terrorism efforts. National counter-terrorism policy lies at the heart of national sovereignty, and will not easily be handed over to the EU.

However, the EU cannot afford to continue without some form of coordinating mechanism for counter-terrorism policy. The question is whether a possible next Mr. de Vries should be called coordinator. An adjustment to the terms of reference for this office is necessary. Other terms might be more appropriate, taking into account the powers that this person will actually have. Negotiations within the Council are ongoing. Whatever the outcome, it is clear that no matter what the title, this office will continue to play a role in managing intelligence cooperation and give a face to European counter-terrorism policy.

8 Interview with Officer of the Joint Situation Center. General Secretariat, Brussels, 16 April 2007.
Recommendations

It is recommended that the position of counter-terrorism coordinator continues to exist, albeit with different terms of reference. Since the Coordinator will not be able to really coordinate, his task might be reduced to facilitating and streamlining EU counter-terrorism policy. The Coordinator should be given the resources and mandate to fulfill this task.

Cross-Pillar Fertilization

Counter-terrorism policy in the European Union is located both within the Second and the Third Pillar. The legal borderline between Second and Third Pillar causes problems because the different strings of decision-making, procedures, and legal instruments which are applicable make any more comprehensive “cross-pillar” action more difficult and cumbersome.9 Thus, EU counter-terrorism policy is fragmented because of its division over the two EU pillars. Overlapping mandates of Europol and SitCen in the area of counter-terrorism further emphasize the rift between the EU’s Second and Third Pillar. No easy solution is available, since counter-terrorism oscillates between the two pillars. Yet the pillar structure of the EU should not stand in the way of effective EU counter-terrorism policy.

It is recommended that the EU does not let its pillar structure and the accompanying practical and legal issues stand in the way of effective counter-terrorism policy. Cross-pillar fertilizations, cooperation and synergy should be stimulated.

7.4 Legal recommendations

Data protection

The EU pays a substantial amount of attention to the protection of fundamental freedoms of European citizens while establishing and maintaining the area of justice, liberty and security. Data protection laws are cited in every Council and Commission decision, communication and framework. The EU entertains its own European Data Protection Supervisor (EDPS).

The balance between privacy and the increased mandate of national and European security bodies has been extensively discussed in other publications. Here it suffices to say that the EU should continue to pay attention to fundamental rights and freedoms, especially concerning privacy in counter-terrorism policy.

It is recommended that the EU continues to ensure the compatibility of its counter-terrorism policy with existing legislation, especially in the field of data protection.

7.5 Technical recommendations

Secure means of communication

The absence of secure means of communication is often mentioned by national intelligence services as a problem in submitting and sharing intelligence at the European level. By this they mean that no secure means of communication exists between many national intelligence services and EU information agencies. Indeed, many databases of national intelligence services and EU institutions cannot be connected without adjustments or secure communication systems are missing.

Several “commercial off the shelf” (COTS) products are available to present information from different sources and different databases in a single, user-friendly platform. Several digital content corporations, as well as publishing houses and the developers of data mining tools have products which could provide partial solutions to this problem.
However, the problems are not only technical. Sometimes the lack of secure means of communication is presented to hide a lack of political willingness to share intelligence. While some technical issues may persist, a much larger problem in exchanging intelligence is the lack of political willingness. Member states remain hesitant to share their sensitive counter-terrorism information directly. Direct access of Member States to each others databases, let alone direct access for European institutions, seems a distant reality.

It is recommended that secure means of communication exist between every EU Member State and every EU information agencies. EU information agencies and relevant EU institutions such as the Council, the Policy Unit and the Commission should also have such secure means of communication at their disposal.

### 7.6 Recommendations concluded

- It is recommended that the EU expands its scope and flexibility of intelligence to an increased number of non-traditional sources and methods to counter current threats to its area of justice, liberty and security. The concept of intelligence-led law enforcement should be engrained in the entire EU intelligence community.

- It is recommended that the EU information agencies fulfill the intelligence function for EU decision makers, and need to be given sufficient resources to perform this role. It is recommended that the EU information agencies deliver better results for national intelligence agencies. Synergy and cooperation between the EU information agencies should be guaranteed. Trust and confidence in EU information agencies should be encouraged and stimulated, for instance through nourishing personal contacts and positive experiences with the agencies for national law enforcement bodies. The principle of availability should be implemented in a way that it can fulfill its promising role.

- It is recommended that the EU develops OSINT at the European level with enhanced vigor. OSINT’s increasing relevance to EU counter-terrorism policy should benefit from improved selection and analysis at the European level.
It is recommended that the EU invests heavily in ‘soft’ measures to stimulate intelligence cooperation. Such ‘soft’ measures can include languages courses, conferences and workshops to nourish personal contacts between intelligence officers, training, recruitment, education and increased mobility of intelligence officers.

It is recommended that the EU intelligence community functions without the development of its own collection capabilities. Its current strong points should be emphasized, by increased national – European sharing. In the future, a scenario could be envisaged where EU information agencies such as Europol or SitCen can task national intelligence agencies with a certain collection task.

It is recommended that the FORINT approach is seriously researched and considered by the EU as a method of stimulating EU intelligence cooperation.

It is recommended that the EU stimulates national intelligence services to specialize, thereby emphasizing and enhancing their strong points. National intelligence services should –in the future- abandon their desire to remain “information-independent”.

It is recommended that the EU maintains a central inventory of all counter-terrorism measures.

It is recommended that the position of counter-terrorism coordinator continues to exist, albeit with different terms of reference. Since the Coordinator will not be able to really coordinate, his task might be reduced to facilitating and streamlining EU counter-terrorism policy. The Coordinator should be given the resources and mandate to fulfill this task.

It is recommended that the EU does not let its pillar structure and the accompanying practical and legal issues stand in the way of effective counter-terrorism policy. Cross-pillar fertilizations, cooperation and synergy should be stimulated.

It is recommended that the EU continues to ensure the compatibility of its counter-terrorism policy with existing legislation, especially in the field of data protection.

It is recommended that secure means of communication exist between every EU Member State and every EU information agency. EU information agencies and relevant EU institutions such as the Council, the Policy Unit and the Commission should also have such secure means of communication at their disposal.
Bibliography

Books


### Articles


● Müller-Wille, B. (2003) SSR and European Intelligence Cooperation Implications of the New Security Challenges and Enlargement (Both EU and NATO) for Structuring European Intelligence Cooperation, as an


- Prospects for a European Common Intelligence Policy, Villadsen, O.R. Georgetown University, 29 November 2000.


EU publications


- Charter of Fundamental Rights of the European Union, Chapter II Freedoms, article 8 protection of personal data. 18 December 2000.

- Communication from the Commission to the Council and the EP on measures to be taken to combat terrorism and other forms of serious crime, in particular to improve exchanges of information - proposal for a Council Decision on the exchange of information and cooperation concerning terrorist offenses, European Commission, 29 March 2004


- COUNCIL FRAMEWORK DECISION of 13 June 2002 on combating terrorism, (2002/475/JHA)


- Hague Program (Council Conclusions) of 5 November 2004 (16054/04, 13 December 2004).


- Preamble of Council of the European Union, Prüm Convention, doc. 10900/05 CRIMORG 65 ENFOPOL 85, Brussels, 7 July 2005.
List of interviews, conferences and missions

Interviewees

For reasons of privacy and confidentiality, personal names will not be disclosed throughout this list. Instead, the names of the departments and organizations that these officers work at are mentioned.

<table>
<thead>
<tr>
<th>Organization</th>
<th>Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dutch Civil Intelligence and Security Service</td>
<td>Officer 1</td>
</tr>
<tr>
<td>Dutch Civil Intelligence and Security Service</td>
<td>Officer 2</td>
</tr>
<tr>
<td>Dutch Military Intelligence and Security Service</td>
<td>Officer 1</td>
</tr>
<tr>
<td>Europol</td>
<td>Officer 1</td>
</tr>
<tr>
<td>Europol</td>
<td>Officer 2</td>
</tr>
<tr>
<td>Europol</td>
<td>Officer 3</td>
</tr>
<tr>
<td>Intelligence Division EU Military Staff</td>
<td>Officer 1</td>
</tr>
<tr>
<td>International Institute for Strategic Studies</td>
<td>Officer 1</td>
</tr>
<tr>
<td>International Institute for Strategic Studies</td>
<td>Officer 2</td>
</tr>
<tr>
<td>Joint Situation Center</td>
<td>Officer 1</td>
</tr>
<tr>
<td>Scottish Tayside Police</td>
<td>Officer 1</td>
</tr>
</tbody>
</table>

Attendance of conferences and workshops

<table>
<thead>
<tr>
<th>Conference</th>
<th>Date and Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>European Security Research Conference</td>
<td>26-27 March 2007, Berlin</td>
</tr>
</tbody>
</table>
## Research Stays

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>27 – 28 February 2006</td>
<td>Europol, The Hague</td>
</tr>
<tr>
<td>8 – 11 May 2007</td>
<td>International Institute for Strategic Studies, London</td>
</tr>
</tbody>
</table>
List of abbreviations

9/11 ......................... 11 September 2001
AWF ......................... Analytical Work File
AIVD ......................... Dutch Civil Intelligence and Security Service
                          (Algemene Inlichtingen- en Veiligheidsdienst)
CATS ......................... Article 36 Committee
CEPOL ....................... European Police College
CFSP ......................... Common Foreign and Security Policy
CIA .......................... Central Intelligence Agency
CIC  .......................... Civilian Intelligence Cell
CIP ........................... Common Intelligence Policy
CLASSINT ................... Classified Intelligence
ComCen ...................... Communications Center of the Council
Commission WMD...... The Commission on the Intelligence Capabilities
                          of the United States Regarding Weapons of Mass
                          Destruction
COREPER ..................... Permanent Representatives Committee
COREU ....................... CORrespondance Européenne
CORTESY .................... COREU Terminal Equipment SYstem
COTER ....................... Counter-Terrorism Working Party
COTS ........................ Commercial Off The Shelf
CT ............................ Counter Terrorism
CTG .......................... Counter Terrorism Group
DG ............................ Directorate General (EU)
ECJ .......................... European Court of Justice
EDA .......................... European Defense Agency
EDPS ......................... European Data Protection Supervisor
EIP ........................... European Intelligence Policy
ELINT ........................ Electronic Intelligence
EMSA ........................ European Maritime Safety Agency
EP ............................ European Parliament
EPICCC ....................... Euroregional Police Information and Coordination
                          Center
ESDP ........................ European Security and Defense Policy
ETA .......................... Euskadi Ta Askatasuna (Basque Homeland and
                          Freedom)
EU ............................ European Union
EUMS ........................ European Union Military Staff
Eurojust ..................... European Union Judicial Cooperation Unit
Europol ..........................European Police Office
Eurosint .........................European Open Source Intelligence Forum
EUSC ..............................European Union Satellite Center
FORINT ...........................Foreign Intelligence
Frontex ...........................Frontières Extérieures
HQ ..............................Headquarters
HUMINT ............................Human Intelligence
IED ..............................Improvised Explosive Device
IISS ............................International Institute for Strategic Studies
IMINT .............................Imagery Intelligence
INTDIV ............................Intelligence Division of the European Union Military Staff
IR ...............................International Relations
IRA ..............................Irish Republican Army
JIT ..............................Joint Investigation Team
JLS ..............................Justice, Liberty and Security
JRC ..............................Joint Research Center of the European Commission
MIVD ..............................Dutch Military Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst)
MoU ...............................Memorandum of Understanding
NATO .............................North Atlantic Treaty Organization
OSINT .............................Open Source Intelligence
PCOTF ............................Police Chiefs Operational Task Force
PLO ..............................Palestinian Liberation Organization
RAF ..............................Rote Armee Fraktion (Red Army Faction)
RELEX .............................External Relations
SGHR .............................Secretary General / High Representative
SIAC .............................Single Intelligence Analysis Capacity
SIGINT ............................Signals Intelligence
SIRENE ............................Supplementary Information Request at the National Entry
SIS .............................Schengen Information System
SitCen ............................Joint Situation Center
TECHINT ..........................Technical Intelligence
TE-SAT ............................Terrorism Situation and Trend Report (Europol publication)
TWG ..............................Terrorism Working Group
UK ..............................United Kingdom of Great Britain and Northern Ireland
UN ..............................United Nations
UNICRI ..........................United Nations Interregional Crime and Justice Research Institute
US PATRIOT Act ...........Uniting and Strengthening America by Providing
Appropriate Tools Required to Intercept and Obstruct
Terrorism Act
US..............................United States of America
WMD .........................Weapons of Mass Destruction
Interview protocol

**Introduction**

Introduction of the interview

Intelligence sharing in the European Union to combat terrorism

Interviewing policy makers and operational personnel

Focused not on confidential information but strategic-level intelligence

Specific focus on informal methods of intelligence sharing

Realistic assumptions about information sharing.

The report of the interview will be subject to your clearance. No personal data will be used: you will not be quoted directly. You will receive a final copy of the report.

**General questions**

Could you tell me about yourself? What is your exact position? Where have you worked before you arrived at your current position?

In your job, how often are you concerned with the exchange of intelligence in the European Union to combat terrorism? Would you consider this topic a central part of your activities?

**Intelligence sharing**

How often are you in contact with European intelligence services such as Europol, SitCen, or INTDIV? With whom are you in contact?

How often are you in contact with operational personnel from national intelligence services?

How often are you in contact with policy makers who are concerned with intelligence sharing as a policy area? With whom are you in contact?
Informal and formal sharing

How do you share important information within your own organization? Do you use formal or informal channels? Could you describe an average exchange process?

If or when you share intelligence with other organizations within your own country or other organizations in different countries, do you mostly use informal or formal arrangements for sharing intelligence? Could you describe an average exchange process?

Do you usually know personally those persons with whom you exchange intelligence? Is this a necessary requirement for you to exchange intelligence? How have you gotten to know these persons? How important are personal relationships in intelligence sharing?

How often do you use formal arrangements for intelligence sharing? Do the formal arrangements for intelligence sharing fit with the daily realities of your job? How easy do you find it to use these formal arrangements? Do you find the procedures quick, reliable and safe?

Do you receive intelligence from other organizations? If yes, in what way? Could you describe an average process of receiving intelligence from another organization?

What type of intelligence do you usually share with other organizations? Do you share individual pieces of intelligence or are you more likely to share analyses and complete reports?

The use of intelligence sharing as a tool for fighting terrorism

Do you think there is a need for more and better intelligence sharing in the European Union, provided its goal of providing security for its citizens against terrorism?

How important do you think intelligence sharing is as a tool for fighting terrorism within the European Union?
**Improved intelligence sharing**

What do you see as the most important problems in intelligence sharing? Please be as specific as possible.

- Legal
- Technical
- Organizational
- Cultural
- Political
- Financial

What do you see as the most promising manner to stimulate more and better intelligence sharing in the European Union?

Is there something that would entice you personally to share more intelligence? Such as a secured communication system, a relationship of trust with other persons in equivalent jobs etc.