Universiteit Leiden

Sandra Diana Will

s1799487

06.06.2017

Master Thesis

Supervisor: Dr. G. M. van Buuren

Second reader: Els de Busser

An Integrated Information Management for Counter Terrorism Purposes within the European Union- Law Enforcement's Perspectives on Information Exchange, Capabilities and Obstacles

A thesis submitted in partial fulfilment

of the requirements for the Degree of Master of Science

in Crisis and Security Management

at the University of Leiden

by Sandra Diana Will

Table of Content

I. Abstract

Although, a lot of academic literature exist concerning the European Union's efforts to implement an 'integrated information management system' for counter-terrorism purposes, there has been little research done to elucidate the practitioner's view in law enforcement agencies. In the light of the pressing need to reveal *how* these officers deal with the uprising tensions between the top-down driven policies and the bottom-up surfaced problems from the member states, this topic needs to get more attention. This research will not merely assess qualitatively what has been done on the process of implementation, boosting the information exchange and intra-agency cooperation from the political-administrative perspective; it will also reveal the practitioners' views and perceptions about the current state of play of formal information exchange. Six police officers were hand selected for semi-structured face-to-face interviews to get an insight in their daily duties followed by recommendations based on their professional experience. According to the findings of this study, most of the practitioners assume that the advancements of the current information architecture are necessary and opportune. Even when they appraise the plans on political-administrative level as more than ambitious.

Doubtless, in the light of the current terrorism threats posed by returning foreign terrorism fighters, the detection of potential 'endangers' needs to be addressed as early as possible to ensure security for the whole European society. Further research to explore these options, should be tackled insistently to prevent the slipping of crucial information through the cracks of security authorities in the future.

II. List of Abbreviations

AFSJ	– Area of Freedom, Security and Justice
AWF	– Analysis Work Files
CIA	– Central Intelligence Agency of the United States
ECTC	– European Counter Terrorism Centre
EIS	– Europol Information System
EIXM	– Communication on the European Information Exchange Model
ENU	– European National Unit
EPE	– European Platform for Experts
EU	– European Union
EU CTC	– European Counter Terrorism Coordinator
Europol	– European Police Agency
FIUs	– Financial Intelligence Units
FIU.net	– Financial Intelligence Unit's network
FBI	– Federal Bureau of Investigation of the United States
IRU	– Internet Referral Unit
PNR	– Passenger Name Records
PWGT	– Police Working Group on Terrorism
SIENA	– Secure Information Exchange Network Application
SIENA CT	– Secure Information Exchange Network Application for Counter-Terrorism
SIRENE	– Supplementary Information Requested at the National Entries
SIS	– Schengen Information System
SLTD	– Stolen or Lost Travel Documents

III. Acknowledgements

The gained experience in the master program ‘Crisis and Security Management’ enriched my professional knowledge with the academic approach in the highly relevant field of security. I recognized that between the two pillars, the professional and the academic approach, there still exist a gap that needs to be overcome. In this regard, I appreciated to be able to broaden my horizon during the studies and to encourage hereafter both sides, the practitioners as well the scholars, to learn from each other for a ‘common response caused by common threats’.

Special thanks to my supervisor, Dr. G. M. van Buuren, for his inspirational comments and constructive criticism. Jelle, thank you very much for your deep interest in my topic and your enthusiasm that kept me motivated and aim-oriented.

However, this thesis would not have been possible without the encouragement by my beloved family. Warm thanks to my parents and my children who had to suffer most the limited time I had for them. Lastly, I would like to express my deep gratitude to my husband, who always believes in me. Micha, thank you so much for your sincere support and patience.

Sandra Will
June 2017

1 Introduction

By the end of 2013, the European Union (EU) was almost spared from any terror attacks that can be linked to the phenomenon of foreign terrorism fighters.[1] Initially, the attack on 24 May 2014 in the Jewish Museum in Brussels, Belgium, carried out by a French national brought a new increased and perceptible terror threat directly to the European Union. [2] This phenomenon or more precisely religiously inspired terrorism added a new dimension to the already existing threats in the EU.[3] It ended up with an abundance of measures on counter-terrorism agendas in the security services of the respective member states. As a well-known reaction on terror attacks, the actors on highest EU political-administrative level called for more data collection and information exchange. The European security actors - in first place Europol[4] - were suddenly confronted with a much more pressing need to exchange relevant counter-terrorism information. Theoretically easy to articulate, but in practice a highly bureaucratic, complex and technical challenge that affected all law enforcement units dealing with the processing of personal data of suspects. The establishment of an 'integrated data management model' capable for information exchange seemed crucial improving the intra-agency cooperation. Especially, in the light of the threat posed by a rising number of religious and radicalised returnees mainly from Syrian conflict zones.[5]

---

[1] The UN Security Council defined in its resolution 2178 the 'foreign terrorist fighters' "[…] as nationals who travel or attempt to travel to a State other than their States of residence or nationality, and other individuals who travel or attempt to travel from their territories to a State other than their States of residence or nationality, for the purpose of the preparation, planning, or preparation of, or participation in terrorist acts, or the providing or receiving of terrorist training, including in connection with armed conflict."

[2] The French national Mehdi Nemouche, 29, spent before the attack more than one year in Syrian conflict zones (The Guardian, 1 June 2014).

[3] According to the Terrorism Situation and Trend report 2014 by Europol (TE-SAT report), religiously inspired terrorism is considered being the major threat within the most European Member States.

[4] Among other European Institutions, Europol is the only one European Union's agency for law enforcement cooperation according to its new Regulation (EU) 794 of 11 May 2016, entered into force on 1st May 2017.

[5] An 'integrated data management concept' is one of the main objectives of Europol's new Regulation 794, entered into force on 1st May 2017. The core principle is that one unified data set will hold all different data types, ensuring at the same time robust security and handling controls concerning the data across relevant Focal Points (FPs) and other applications.

The EU offers a wide range of competent security authorities which are engaged in the counter-terrorism field, even when the implied powers differ from one member state to another. Whereas, in several states the responsibility is in the hands of law enforcement, it will be combatted in other states in intelligence services, but what they have all in common is that each competent authority has often its own cooperation modalities. The European Police Agency, Europol, is the main law enforcement centre for the collection and analysis of counterterrorism-related information on EU level. Since 1994, Europol serves as the main information hub for the law enforcement agencies in the member states and supports with coordination of operational actions and expertise. [6] One of Europol's objectives is to serve as a platform of first choice for the member states, giving them the opportunity to share strategic and operational information via secure and user-friendly information exchange facilities (Brown, 2010, p. 147). The implementation of the European Counter Terrorism Centre (ECTC) in January 2016, more precisely the implementation of the first common centre for counter-terrorism efforts on EU level, was a response to the terror attacks occurred inside the EU and the increased number of returning foreign fighters from conflict zones (ICCT, April 2016). [7] Ever since, the ECTC needs to deal with an increasing amount of counterterrorism-related data contributed by the member states, whilst at the same time practitioners claim that the used systems are solely in part connected, others not even appropriate for information exchange.

The EU Counter-Terrorism Coordinator (EU CTC) Gilles de Kerchove, who has been appointed on 19 September 2007, has a coordinating and supporting role for the work of the EU Council in all counter-terrorism issues embracing the monitoring of the implementation progress of the counter-terrorism strategies (EU CTC, September 19, 2007). Its role can be described as rather limited, because the main powers remained with the EU Council itself and the primary responsibility on national level of counter-terrorism issues was still lying with the member states (Monar, 2015). Nevertheless, essential efforts have been done to push the implementation of tools enabling the formal information exchange beneficial for all member states (Council of the European Union, December 2016). Moreover, the increased need of secure information technology for intra-agency exchange has become a core business for EU counter-terrorism efforts, as well as a crucial precondition for an integrated information

[6] Europol was established on 3th January 1994, first in the form of the Europol Drugs Unit.

[7] An EU-wide estimate by the ICCT in 2015 revealed that the number of foreign terrorist fighters is still high with 3700 within the EU, whereas the majority with 2800 come from merely four countries, Belgium, Germany, France and The United Kingdom (ICCT, April 2016).

management (Council of the European Union, December 2016). However, the dragging implementation of systems in the member states lead to a change of thinking; instead of new calls towards accelerating the implementation process, the EU CTC discussed new ideas that should include a 'practitioner-centred approach' considering their point of views and recommendations (Council of the European Union, May 2016). With this said, it prompts the question whether the policy and the practitioners follow same objectives? Are they actors with the same vision and are they aware of the different obstacles they need to face in their daily work? In public awareness, merely the policy's objective has been articulated: to establish a broad interconnected and integrated information management system that ensures the interexchange of personal data, which can further be used to detect potential terrorists before an attack will occur (Council of the European Union, 2016). But probably due to the lack of the practitioner's views and ideas, the stalled implementation process cannot be solved effectively, embracing the imbalance of technical equipment in the member states, the domestic obligations and legal rulings but also the mistrust against each other to share information and the missing safeguard for sensitive data.

In the light of several reported failures concerning slipped information through the cracks of security services, it raises the question why these services were not capable to quickly deal with the information via the used IT-systems in the past (Deutsche Welle, 2017 January 18)? Moreover, it prompts the questions whether law enforcement agencies in general have the right tools, if these tools are appropriate for information exchange and more important if the police officers on the spot in the member states have access to it? Even when several stories of successful information exchange repose on informal exchange through personal known communication channels (Travis, 1998), this research will concentrate on the formal information exchange with technical means. The governance of security is nowadays more complex, huge due to the masses of collected data which is closer linked to formal information exchange than ever before. Since the formal information exchange is a relatively unexplored field in the governance of security, this thesis is devoted to a deeper research on *how* the practitioner's views align with or differ from the top-down driven information management systems set out by the European Union.

1.1 Research Questions

The purpose of this study is to grasp the empirical reality on law enforcement practitioners and offer a deeper insight how the top-down driven information architecture from the political-administrative level is related to the real-life scenario on working level. Therefore, the main research question and the sub-questions for this master thesis are:

How do law enforcement practitioner's views align with or differ from the top-down driven information architecture by the European Union and how can this be explained?

1. What do law enforcement practitioners conceive as an effective information exchange based on technical means, advancing the detection of terrorists within the European Union?
2. What do law enforcement practitioners view as the primary barriers for an effective integrated information management?
3. To what extent does the practitioner's view concerning the barriers differ from the policy's top-down perspective?
4. What recommendations do the practitioners name improving the policy and practice of the information architecture by the EU?

The sub-questions above concentrate on specific issues and its results help to answer the overall main research question. The first sub-question aims to identify what practitioners appraise as an effective information management. Whereas the second sub-question will focus on the main barriers which hamper the way forward from practitioner's perspective. Followed by the third question which will reveal to what extent the policy's perspective differ from the latter. The last sub-question will focus on recommendations named by practitioners to achieve a well-performed information management.

1.2 Societal and Scientific Relevance

Twelve persons killed and fifty wounded, that is the sad episode of one of the last terror attacks on 19 December 2016 during a Christmas market in Berlin, Germany. A bloody attack carried out by a radicalized jihadist who was already on the radar of more than 40 German authorities or agencies. Whether the incriminating information on him could not be connected nor the suspect known as potential terrorist could be arrested beforehand.

With this said, the societal relevance is on the dice. The governance of security is nowadays more complex and closer linked to information exchange with technical means than ever before. The more masses of data can be collected, the more important is the need to link information and wash them against criminal records. These terror threats affect all citizens and the prevention of it ensures a life in a more secure Europe. Findings of this research can show the 'practitioners-centred approach' and finally support decision-makers on political level who are encouraged to tackle new approaches for an improved detection system revealing potential terrorists.

In the multidisciplinary field of 'crisis and security management' many studies have been conducted to reveal the main challenges and obstacles for the slow progress in information-sharing (Den Boer, 2015; Brown, 2010; Müller – Wille, 2008; Walsh, 2006). They mainly concentrate on the question on how the strategies and the improvement of counter-terrorism measures can be measured and on how these are related to the accountability and transparency of collecting and sharing data. In addition, several scholars claimed that mistrust and the low safeguard for classified information are the main barriers to progress (Walsh, 2006; Nelson, 2011). Therefore, this master thesis will also explore the current state of the art of contemporary safeguard standards and its current level of trustworthiness. However, what is entirely missing in the literature is the view from the practitioner's perspective, from officers who are dealing with criminal records on daily basis. According to the academic literature, a closer connection between research and practice can be highly valued by practitioners but also the scholars can learn more about the relevance of their own research (Tushman, 2007, p. 134). Moreover, this knowing-doing relationship can lead to more effectiveness in the work of the scholars (Tushman, 2007, p. 134). Therefore, one of the main objectives of this study is to link research and practice as close as possible. The outcome should have an impact on further steps in 'practice', establishing new approaches based on the practitioner's views. Against this backdrop, the findings of this research will contribute to the existing body of knowledge and fill a gap in the academic literature.

1.3 Overview of Research Project

After the topic has been introduced that is underlying this master thesis and explained related to the societal and scientific relevance, the second chapter will follow with the focus on the main existing literature to establish the theoretical framework. In the third chapter, the contextual framework will provide insights in the European Union's information architecture and technical capabilities of the contemporary used IT-systems and the current state of play of implementation progress. The fourth chapter will give an overview of the used methodology to better understand the data collection process and the methods applied in this study. Followed by the critical analysis in the fifth chapter, in which the two fronting 'visions' will be compared and analysed. In the conclusion, all findings and recommendations of this study will be presented as well as potential upcoming issues that can be elucidated in further research.

2 Theoretical Framework

The second chapter will set out the theoretical framework for this thesis. First, the EU's role as a counter-terrorism actor will be described, followed by thoughts in the academic literature about the process of 'Europeanization' and the convergence in this domain. Then, Europol's role as an important European security actor will be outlined and further the tensions that arise between the EU and the practitioners working in the security agencies. Furthermore, it will be illuminated the academic discussions about 'better instead of more information exchange' and the need for a common response to the terror threats.

2.1 The European Union as a Counter-Terrorism Actor

One of the main objectives in the Treaty on the European Union is the provision of a high level of security for all citizens within an Area of Freedom, Security and Justice (AFSJ). [8] Regarding the security strategies by the EU at large, it can be argued that the developments of the EU's internal and external strategies have been proven to be more capability-driven than strategy-led, resulting in a 'capability-strategy' mismatch (Schroeder, 2009, p. 492). This process has been observed in several policy arenas such as counter-terrorism, crime-fighting and common defence embedded within the complex EU security architecture. According to Schroeder (2009), the different EU actors follow diverging strategic aims with in part overlapping agendas leading to the emergence of fault lines in the security policies (p. 486). More precisely, the EU's capabilities emerge before their member states had discussed and formulated the final targets they want to achieve (Schroeder, 2009, p. 487). Thus, the EU's security strategies so far appear more peculiar because their priorities were predominantly emerged by stealth, rather than by design (Schroeder, 2009, p.487). In this context, it should be mentioned that often security strategies ended up in low-profiled concept papers, instead of being implemented on national-administrative level (Schroeder, 2009, p. 487). With this said, it is not remarkable that these deficiencies in the EU's top-down steering policy process had an impact on the dragging implementation process within the EU's Counter-Terrorism Strategy.

[8] The Treaty on the European Union stipulates in Title V the functioning of the European Union which ensures the free movement of persons and offers a high level of protection to citizens. The creation of the AFSJ is based on the Tampere (1999-04), Hague (2004-10) and Stockholm (2010-14) programmes (EUR – Lex, Access to European Union Law).

The fight against terrorism can be qualified as one of the most prominent aims among other objectives in the EU's AFSJ. In 2005, the EU's Counter-Terrorism Strategy has been adopted aiming at combating terrorism globally and focussing on four main pillars: prevent, protect, pursue and respond (European Council, 2005, p.3). Within the third pillar, under the pursuing aspect, the strategy formulates under No. 27 specific objectives that should be approached as follow:

"[…] To move from ad hoc to systematic police cooperation, an important step will be developing and putting into practice the principal of availability of law enforcement information. In addition, the development of new IT-systems such as the Visa Information System and the next generation Schengen Information System, while safeguarding data protection, should provide improved access to those authorities responsible for internal security thereby widening the base of information at their disposal. Consideration should also be given to developing common approaches to the sharing of information on potential terrorists and on individuals deported for terrorism-related offences" (European Council, 2005, p. 13).

With this said, the EU's Counter-Terrorism Strategy stipulates the improvement of cooperation and intelligence-sharing, an ensured access for all who are engaged for internal security within law enforcement, meaning in the first line Europol as the main European security actor to combat terrorism – alongside Eurojust and Frontex. [9] The EU Counter-Terrorism Coordinator, Gilles de Kerchove, who has been appointed on 19 September 2007, is in charge for the coordination of the EU Council's work in all counter-terrorism issues embracing the monitoring of the implementation progress (European Union High Representative, 2007). Despite of his key position as the EU's chief diplomat in counter-terrorism, the main power remained in the hands of the EU Council (Monar, 2015). Moreover, he has been far away from receiving any real coordination powers (Monar, 2015, 343). Nevertheless, he played an increasing role in the external counter-terrorism domain, especially in the efforts enhancing the capabilities in the third countries (Monar, 2015). Due to his media attention through interviews he became the most visible 'face' of the EU's international role in counter-terrorism (Monar, 2015, p.344). The launched implementation reports by the EU CTC show its exhausting efforts pushing the implementation process in the internal counter-terrorism domain, specifically in the field of

[9] Eurojust provides detailed judicial analysis with its Terrorism Conviction Monitor (TCM) whereas Frontex is primarily responsible for monitoring migratory movements into the EU (Den Boer, 2015).

information-sharing, cooperation in line with the multi-agency approach, but also intra-agency approach with third countries (Council of the European Union, 2016). Although, acknowledging these efforts, its success could be much more. The reasons explaining why the implementation process of EU policies got stuck might have been diverse, but the main explanation described in the literature is that "[…] the Union does not have a 'normal' government at the supranational level with all the requisite powers, competences, and hence, capabilities of regular a government; it is not a federal European state" (Zimmermann, 2006, cited in Kaunert, 2010, p. 653).

Indeed, the overarching assumption in the academic literature has been formulated by Monar (2015) who states that the European Union's role as a Counter-Terrorism actor since the 9/11 attacks in the United States, has been characterized by alternating progress and constraints (p. 333). Furthermore, he argues that the main problems are the lack of operational capability, its institutional complexity and obstacles in cross-policy coordination (Monar, 2015, p.333). Concerning one of the above-mentioned progresses, the EU's efforts towards capability-building in third countries can serve as one example providing a win-win situation with a doubled positive effect (Monar, 2015). The improved capacity in a third country ensures on the one side a reduced counter-terrorism threat and on the other side will this country abroad be an effective partner in cooperation in counter-terrorism areas (Monar, 2015). As opposed to this, considering the constraints, the EU has undertaken parallel approaches to tackle reforms of the security and judicial systems in third countries. Although, it was still engaged in the process of capacity-building (Monar, 2015, p.353).
Noteworthy in this context is the view to the wide range of counter-terrorism measures that have been officially implemented, but their fully adaption in the member states is still fragmentary and dragging on working level (Schroeder, 2009; Oliviera Martins & Ferreira-Pereira 2014, Argomaniz et al, 2015). Another suggestive (more negative) remark was made by Bures (2012) when he referred to the European Union's Counter Terrorism Policy as nothing more as a 'paper tiger'. He pinpoints exactly the problem that is underlying this master thesis. To draw more attention to the main obstacles that slow down or even disrupt the whole implementation process and let the EU as a Counter-Terrorism actor become a 'toothless tiger'.

Conclusively, the counter-terrorism role has been proven as politically and legally more subsidiary, compared to that of its member states (Monar, 2015, p. 333). Indeed, often the policy measures are merely declared on European political level but their implementation on the

operational level in the member states is lacking. Therefore, this thesis will address this divergent logic, more precisely the opposing logic of the political-administrative level on one side and the practitioners level concerning the practicality on the other.

2.2 Uneven 'Europeanization'

With regards to an obvious gap between the declaration and implementation, it prompts up the question about the level of already achieved convergence in counter-terrorism. This implicates that the process of convergence may also be explained in the light of 'Europeanization' theories. There is a huge amount of literature in the field of 'Europeanization' and its approaches and applications elucidating specific problems are diverse. Although, this thesis will neither analyse the level of convergence nor elucidate the dimensions in the Europeanization process, the links to the top-down and bottom-up dynamics of European policy should be mentioned helping to understand the reasons for an adaption or non-adaption by the member states. Due to the diverging definitions, this thesis will use the most appropriate one which describes the here elucidated dynamics best. A well-known definition is offered by Radaelli (2003), who describes Europeanization:

"[…] as processes of (a) construction (b) diffusion (c) institutionalization of formal and informal rules, procedures, policy paradigms, styles, 'ways of doing things' and shared beliefs and norms which are first defined and consolidated in the making of EU decisions and then incorporated in the logic of domestic discourse, identities, political structures and public policies" (Radaelli, 2003, p.30).

Another popular definition offers Börzel (2002), who states that the process of Europeanization is a two-way process, including a 'top-down' and 'bottom-up' dimension which explains the developments of European institutions affecting the political and procedural mechanism of the member states (p.195). According to the literature, one effect of the top-down driven EU legislation may be that the organizational structures and working procedures on national level will slowly converge because they obtain regularly stimulation by the EU (Fennell et al., 1995, cited in den Boer, 2015). Another factor for policy convergence can be similar policy problems that require the same reaction by national states (Bennett, 1991, cited in Knill, 2005).

Connecting at large the terms of these dimensions with the study, the top down-dimension can be understood as the regulations, procedures and declarations by the political-administrative level of the European Union, whereas the bottom up-dimension attaches the dragging process

of adaption on national level. According to Börzel (2002), national governments strive to minimize the costs that may arise due to the implementation of European regulations in their home constituencies (p.194). This generates an 'adaptional pressure', resulting from the divergence between the national and the European level and this leads to a specific mechanism: The higher the divergence, the higher is the pressure to adapt to the European level (Börzel und Risse, 2003). However, to understand better the focus of this study, it is important to break down these top-down and bottom-up dimensions more in-depth, because these dimensions are acting on 'lower' levels, too. More precisely, the member states which set out the EU-policies (top down-dimension) and the practitioners on working level who are confronted with the adaption of these policies (bottom up-dimension) (Council of the European Union, April 2016). Several documents by the EU CTC addressed the most pressing difficulties - a bunch of unfocused measures and resulting problems in terms of practicality for the practitioners (Council of the European Union, 2016). Deeming these shortcomings, this thesis will pay attention to the problems in terms of convergence and the still resisting gap between the political-administrative level of the member states and the level of practitioners.

Conclusively, the process of Europeanization with its top-down and bottom-up dimensions can be observed on different levels among several actors within the European Union. Although, Knill (2005) states that cross-national policy convergence can simply be accelerated by transnational communication and information-sharing (p. 770), the reality within the lower levels of these days demonstrates, that it is easier said than done. Convergence between member states and practitioners is still lacking and needs to be approached with efforts from both sides. However, despite of the fact that convergence tends to be more selective than embracing all administrations, the efforts should be appreciated insofar that "[…] in the field of counter-terrorism there has been unquestionable distinctive national patterns of institutional adjustment, and thus one could speak of an uneven 'Europeanization process' (Den Boer, 2015, p. 386).

2.3 Europol as a prominent European Security Actor

Within the European Union's security architecture, the European police agency can be identified as one of the main connectors between the European Union and the member states. Indeed, Europol has almost the same problems as the EU's policy in general is facing in the field of counter-terrorism. Acting on the interface between the incoming orders by the EU and the uprising problems within the member states, Europol should be able to provide a

comprehensive overview about the current situation of the implementation status of counter-terrorism measures.

Nevertheless, in the light of the current terror threat by a new dimension of international jihadist terrorism[10], it is remarkable, that Europol's role as one of the prominent European security actors has proven by most scholars to be limited (Müller-Wille, 2008; Bures, 2016; Monar, 2015, Kaunert, 2010). Against this backdrop, there are only a few who value its achievements regarding the great strides towards increasing integration and encouraging cooperation between member states since 9/11 (Zimmermann 2006, cited in Kaunert, 2010, p. 653). Kaunert (2010) elucidated in his research the international 'actorness of Europol' in the field of counter-terrorism. According to him, the relationship between Europol and the member states is based on two main components ensuring the connectivity between national law enforcement agencies and Europol (p.655). First, the network of liaison officers, meaning that every state has sent at least one officer to Europol and the connection to their home country will be hold through the European National Unit (ENU) in the member state. And second, the Europol databases that ensure the interconnection via formal information channels (Kaunert, 2010, p. 655). However, despite of Europol's well-performed connection architecture with liaison officers who ensure a close connection to the member states, Kaunert (2010) argues that Europol is still considered as a weak counter-terrorism actor due to the 'lack of supranational powers' delegated under the terms of the EU treaties and the 'lack of trust towards Europol' by the member states (p. 656). Explained in more detail, the missing supranational powers based on the lack of operational powers and the mistrust is caused by several related factors: (1) the different political, judicial and administrative framework in each member state; (2) the precondition that some member states delegates counterterrorism to the police others to intelligence services; (3) the general scepticism against the centralisation of counter-terrorism efforts in Brussels (Kaunert, 2010, p. 656).

These factors have definitively an influencing effect on information-sharing with Europol. Thus, it is not surprising that Müller-Wille (2008) argues, "[…] everything what Europol has

[10] With the 'Terrorism Situation and Trend Report 2016' by Europol, the term 'jihadist terrorism' is replacing 'religiously-inspired terrorism' and the earlier used term 'Islamist terrorism' in TE-SAT reports because of the opportunity that crimes that are committed by a fanatic minority can be related to the religion of Islam with millions of faithful. According to the TE-SAT 2016 report, 'Jihadist terrorism' is considered as the major threat within the most European Member States.

produced, has been produced on national level before, thus the motivation for the EU member states to contribute intelligence to Europol is rather limited" (Müller-Wille, 2008, cited in Bures, 2016, p. 63). In addition, it has been argued that despite of a growing frequency and scope of contacts between national and EU institutions, there is little evidence for more convergence towards a common institutional model (Harmsen, 1999, cited in den Boer, 2015, p.386). The member state's administrations have mostly retained their distinctive structures and operating procedures (p.82). Therefore, Europol has either operational or strategic agreements with states and third countries to obtain information, covering the EU at large identifying national partners for common counter-terrorism cases [11](Monar, 2015, p. 346). And even this cooperation-policy of Europol did not follow a standardized approach according to Monar (2015). These incentives for information exchange were more initiated on a case-by-case basis, depending on the capabilities and interests of member states and cooperating third countries (p. 352). However, den Boer (2015) validates it as an advantage that Europol is regulated by a legal instrument and it is subject to control by EU-institutions (p. 407). That could have an important aspect for its trustworthiness for the member states in the future.

Consequently, despite of Europol's wide network of cooperating member states and third countries, Europol and the member states were not yet able to overcome the grievances regarding the implementation of an effective integrated information management system as required by the EU' Counter-Terrorism Strategy (Council, 20 December 2016). As Walsh (2006) stated, it is not enough to merely establish institutions, the more important it will be - especially for Europol - to overcome the mistrust among each other. Moreover, the awareness-raising is important to recognize two different stages for 'cooperation', with specific cooperation modalities within law enforcement agencies but also between law enforcement and intelligence services. Due to the large amount of academic literature concerning the perspectives of the EU's policies, the central question of this thesis is how the practitioners at Europol view the policy approaches from highest political level and what they identify as the main barriers that slow down the implementation process on working level.

[11] Operational agreements allow the exchange of personal data as opposed to strategic agreements which allow merely general strategic data (retrieved from https://www.europol.europa.eu/partners-agreements/operational-agreements and https://www.europol.europa.eu/partners-agreements/strategic-agreements).

2.4 Tensions between the Supranational Actor EU and the practitioners

On 30 September 2016, the EU Counter-Terrorism Coordinator, Gilles de Kerchove, addressed during a speech at the European University Institute in Florence to the challenges for counter-terrorism at EU level: "[…] jihadi attacks reveal the EU failure of imagination." Further he argued that the member states still have "to improve the sharing of data" – meaning sharper data analysis. The member states need to overcome the mistrust climate that de Kerchove describes as a "Cold War mindset", by feeding and using more the existing databases and ensure their interoperability (Kerchove, 30 September 2016).

Already in 2006, it has been argued in the academic literature that the sheer establishment of European Institutions as the European reaction to terror attacks, is not enough to overcome the main barrier such as mistrust in each other that slow down a closer cooperation and the intelligence-sharing process (Walsh, 2006). According to Walsh the concept of intelligence-sharing can be described as follows: "[…] intelligence is the collection and analysis of open, publicly available and secret information with the goal of reducing policy-makers' uncertainty about a security problem.[12] Intelligence-sharing occurs when one state – the sender – communicates intelligence in its possession to another state – the receiver" (Walsh, 2006, p.626 - 627). In addition, several studies concentrate on the adaptive processes towards more intelligence-sharing and interoperability as well as the harmonization between law enforcement agencies and intelligence services (Bures, 2015; Walsh, 2006; Müller-Wille, 2008). According to Walsh (2006) an intra-agency information exchange requires an open willingness to share information. Outright, 'mistrust' based on divergent policy interests or simply unconscious can be named as one of the main key barrier to an effective information-sharing (Walsh, 2006, p. 626). Generally intelligible, even when intelligence cooperation requires the need to provide sensitive data but without knowing for which use (Paulussen, 2016). This obstacle of mistrust needs to be redressed. An intra-agency intelligence-sharing requires an open willingness to share information, especially when you need to handle sensitive and classified data in the field of counter-terrorism. The non-existence of this willingness to become partners in an information-sharing arrangement is not new and goes back to the time of the 9/11 attacks in the

[12] In the academic literature, there are different definitions for 'intelligence'. M.M. Lowenthal (2009) considers different definitions for intelligence. It can be a process as described by Walsh, an organization or the product itself. Europol defines intelligence "[…] as knowledge (processed information) defined for action" (Europol website).

United States. Before this bloody attack in September 2001, the approach towards cooperation between US-intelligence services and law enforcement agencies were identified as the classical case of incapacity of information-sharing (Nelson, 2011). [13] The evaluation of this terror attack showed exemplarily the failures of information-sharing mainly caused by mistrust and the lack of awareness of the need to share information (National Strategy for Information Sharing, 2007).

Based on Oldrich Bures' research on Europol in 2016, he made harsh critics on Europol's promises to advance the fight against the terror threats with a better information-sharing and how it approaches convincing the member states to comply with the arranged measures (Bures, 2016, p. 58). Further Bures (2016) argued "[…] that despite the need for borderless intelligence sharing as a response to borderless terrorism, Europol is highly unlikely to become a genuine intelligence agency in the foreseeable future" (Bures, 2016, p. 57).

Based on experiences in the field of policing and immigration, some scholars argue that stability and reproduction of institutions are more likely when an increasing number of actors appreciate the means and products of these institutions (Turnbull, P. and Sandholtz, W., 2001, cited in Argomaniz, 2010, p. 22). This implicates that the more actors appreciate the products of an institution (in the case of Europol its reputation for analytical reports and operational support), the more it leads to trustfulness and stability of the institution itself. With this said, these developments can be identified as the classical 'chicken-egg' dilemma. On 13 May 2016, the EU CTC informed the member states of the state of the use of Europol and its databases, in the context of the fight against terrorism (Council of the European Union, 2016). It shows exemplarily the standard procedure; member states that understood the potential added value of Europol are keen to intensify the cooperation whereas other member states are more reluctant due to a lack of experiences with Europol's services at all. More precisely, it has been argued that solely the member states most affected by the foreign fighter phenomenon recognize the added value and this is unfortunately still a minority of member states in single figures, that make use of Europol (Council of the European Union, April 2016, p. 2). These experiences can be useful background knowledge for the decision-making process on EU political level enhancing new counter-terrorism mechanism for information exchange.

Further tensions can be identified among the practitioners in different security services,

[13] In the first line the missing cooperation between the CIA and the FBI.

meaning between law enforcement and intelligence services. The still remaining reluctance on both sides and the lack of technical means to ensure a secure information-sharing still hamper Europol. The problem is multi-layered and described as cultural resistance, at least in several member states where the cooperation between these security services has no traditional roots. According to Bures (2016), it is "[…] primarily due to the persistence of nationality in international policing and intelligence (p. 61). Even when several EU regulations include obligations to exchange information, the decision-making power to do so, is still in the responsibility of the member states (Bures, 2016). Noteworthy in this context is to mention, that intelligence services use their own information-sharing channels. For instance, the Police Working Group on Terrorism (PWGT) can be named as the oldest network ensuring the sharing of more sensitive data than Europol is able to handle (Council of the European Union, March 2016)[14]. As opposed to this, even when the PWGT ensures a level of 'secret', compared to Europol which still has 'confidential' (one level lower), the PWGT merely is a network based on informal information exchange. However, the planning provides that the communication network will be hosted by and integrated into Europol in the future (Council of the European Union, March 2016, p.14).

As mentioned before, another obstacle against a successful formal information-sharing is the lack of standardised procedures guaranteeing that classified information is safeguarded (Nelson, 2011). As Nelson pinpoints, the improvement of technical solutions should be used to the resolution of terror threats (Nelson, 2011). Due to the huge amount of technical means for data collection, supplemented with changing security threats by loose networks and individuals, the need for interoperability and harmonization between criminal and intelligence databases are more important than ever (Den Boer, 2015, 407). Regarding the policy, Bures criticises that often the policy is not precise enough to name exactly which information channels should be used for the exchange (Bures, 2016, p. 60). Thus, the way forward should be focused on a technically improved more secure sharing between the competent authorities in the member states and to clarify which channels or tools should be used (Nelson, 2011; Walsh, 2006, p. 626). Meaning that the overarching implementation of tools and IT-systems should inherently be accompanied during the whole adaption process to ensure an added value for all actors in

[14] The Police Working Group on Terrorism (PWGT) was established in 1976 as an informal network between The Netherlands, Germany and Italy aiming at information exchange on terrorism issues. Since 1979, the members are all EU member states and Norway and Switzerland
(retrieved from http://dip21.bundestag.de/dip21/btd/17/131/1713197.pdf).

the field of counter-terrorism.

To sum up, we can assume that the establishment of new agencies like Europol, Eurojust and Frontex is not enough to improve information-sharing (Walsh, 2006). By the way, this presumption was already made in the year 2006 which shows that it was obviously a high controversial discussed topic after the 9/11 attacks and even a complicated process that needed to be accelerated, accompanied and continuously pushed from political side. The need for information-sharing popped up again as a topic of highest priority in the light of the committed attacks since 2014 in the EU. But with the distinction, that nowadays the law enforcement agencies do not merely need to cooperate closer with other law enforcement authorities but rather more with intelligence services. Further, all security services need to deal with a lot more masses of data due to an increased capacity of data collection resulting on the technological development in the last decade. With this said, the above-mentioned tensions between the different actors require a more deeper understanding in the light of the need for an efficient data processing and formal information exchange.

2.5 Common threat requires common response?

Whereas in 2006, a study showed that the perception of the terror threat is based on various experiences and perceptions resulting that there existed no 'common threat perception' in the EU (Bakker, 2006, p. 54), one should take into consideration that this might have been changed over the years. As opposed to this, a survey conducted by the European Commission in April 2015, showed that there is a rising concern about security threats especially on terrorism and religious extremism. According to the survey, half of the participants view terrorism as the most challenging threat to the security of the EU, compared to merely one-third of the respondents ask four years ago in the year 2011 (MEMO Brussels, April 2015).[15]

The threat perception has further influence on the management of the security services architecture within the EU. Several scholars elucidated in the years 2005 – 2010 the improvement of intelligence sharing among the EU institutions with a focus on Europol. They raised the question why the already in this time-period increased threat perception from international terrorism did not have more effect to create an overarching institutionalized EU

[15] During 21th and 30 March 2015 the survey had been carried out in 28 EU Member States with 28.082 participating respondents.

intelligence service as a response (Müller-Wille, 2008, p.51)? In the light of the coherence between threat perceptions and cooperation focusing on information exchange, den Boer stated that a persistent threat of domestic terrorism has a strong converging influence how to deal with threats in nation states and thus it can have a push-factor for information exchange (Den Boer, 2015, p. 400). Having this in mind, the increased terror threat perception within the EU, added with concerns that returnees from conflict zones and isolated individuals may turn into violent extremists or even lone actors, have (already) contributed to the rise of and the need for interoperability between databases of law enforcement and intelligence services (Den Boer, 2015). Thus, the common threat arisen from international terrorism requires definitively a common response based on political justification (Monar, 2015, p. 335).

2.6 Better instead of more information exchange!

Far less attention has been paid in the literature to the increasing information flow and the collection of masses of data for the purpose to detect potential terrorists. Even though, several studies elucidated the challenges for the governance of this mania of the collection of masses of data, its analysis and exchange, they focus more on aspects such as accountability and transparency in the light of the protection of personal data or on various levels of oversight (Den Boer, 2015, Bures, 2016). Other scholars argue that the expansion of mass surveillance instruments have led to a fast-growing amount of data and finally to new challenges for the governance of surveillance (Den Boer & van Buuren, 2012). Several new technologies have been implemented due to the digitalization, resulting in the shift from 'databases to security clouds' (Den Boer & van Buuren, 2012, 86). In the last decade, numerous security databases have been established for different purposes, in different institutional context and at various times, and have led to a diverse information architecture within the member states (Den Boer & van Buuren, 2012). Added with the new technical opportunities it prompts the question, whether the collected data will be generally washed against criminal data bases and how the data will be used and from whom (Kuipers, 2008, cited in Den Boer & van Buuren, 2012)? [16] This assumption has also been touched upon by Kaunert (2010) who argues that the increase of police operations and investigations that generate masses of data arise questions in the field of data protection and human rights (p. 667). Moreover, due to the (obviously existing)

[16] Kuipers arises this question specifically in the light of the collected data with the Passenger Name Records (PNR) agreement.

interconnected databases and the accessibility to a broad range of criminal investigations, intelligence and surveillance objectives, it arises the question why several information regarding terrorists in the last years could not be linked to each other. Therefore, it can be concluded that information-sharing should be approached better instead of more (CEPS, 6 April, 2016).

2.7 Conclusion

To sum up, it can be argued that the EU as the main counter-terrorism actor has been proved to react more event-driven based on its capabilities instead of acting grounded on a developed strategy. Although, the EU declarations had been pointed at the right direction, their progress of implementation leaves much to be desired. The resulting declaration-implementation gap affects mainly the administrative actors encouraged to adapt the declared measures and shows that in terms of convergence further efforts need to be done. Particularly, Europol as the most prominent actor is facing the challenges. On the one side, it serves as an ideal place from where the accumulated measures by the EU can be communicated to the member states aiming at replying to the common terror threats. On the other side, the masses of collected data needs to be coordinated and analysed and exactly this prompts up the question, to what extend the information collection and sharing is manageable. More precisely, does it make sense to collect masses of data or would it be better to have qualitatively higher valued data? With this said, this thesis will draw attention to the practitioners working at Europol to elucidate their view to the top-down driven information architecture by the EU. To reveal their proceedings with data collection and information exchange and finally, to better assess their capabilities to detect potential terrorists in the EU.

3 Contextual Framework

This chapter will provide an overview of the currently applied information management system in the EU on counter-terrorism issues. Further, the mainly used IT-systems will be explained regarding their technical capabilities and appropriateness for interconnectivity which is formulated to be the main idea of an 'integrated information management system'. Finally, the current state of play of the implementation progress will be given to be better able to distinguish between released measures, measures in progress and implemented measures.

3.1 The EU's Information Management on Counter-Terrorism

The need for a fully implementation of counter-terrorism measures set out by the European Council has never been before so urgent than today. The achievements so far in the field of cooperation and information exchange are difficult to identify in the jungle of policy documents, regulations, recommendations and proposals, within an even more confusing group of EU's institutions engaged in the counter-terrorism domain. Generally speaking, it can be described as a 'messy order or orderly mess'. Insofar, it prompts the question whether it can be named a real advancement in comparison to the beginnings of cooperation, started with the TREVI-process in 1979. [17] Indeed, a large part of amendments have been described in the past more 'attack-driven', since the 2001 attacks in New York, the 2004 bombings in Madrid and 2005 in London. Notwithstanding, the new wave of religiously inspired international terrorism since 2013, has contributed to an increasingly common approach by the European Union, embracing all institutional actors and member states. Even though, there is still a lot more to do. Obstacles such as the persistence in national thinking, the lack of trust and supranational actorness by the EU to push the implementation process, are still the topics we need to deal with (Bures, 2016).

With the implementation of 'The Hague Programme' in 2005, the European Council named the prevention and the suppression of terrorism as a key task and put for the first time more emphasis on a closer cooperation among the member states, particularly concerning technical assistance, training and the exchange of information (Council of the European Union, The Hague Programme, p. 3). Additionally, it introduced the principle of 'availability' as a guiding

[17] The TREVI group has been established in 1976 by 12 states of the European Community (EC) aiming at information exchange on topics such as terrorism and policing in the EC.

concept for law enforcement, meaning that any relevant information that is available in one member state should be made accessible for any other member state (Council of the European Union, 2005). Complementary, the European Council adopted in 2008 the 'Prüm Decision', containing rules for police cooperation and introducing specific proceedings for a fast and efficient information exchange on specific crime areas (Council of the European Union, 2008)[18]. The following 'Stockholm Programme (2010 – 2015) emphasized the need for coherence and a further development of law enforcement cooperation mechanisms (Council of the European Union, 2010). Based on the Prüm Decision, in 2012 the European Council set up the project group, 'Communication on the European Information Exchange Model (EIXM)', that served as a monitoring system for the EU information exchange landscape and worked out recommendations to improve the efficacy and application of already existing cooperation systems. In 2014, an external study had been requested by the European Commission, evaluating the implementation status followed by the recommendations of the EIXM. The study revealed that the most essential efforts had been done by the member states and by Europol, but stressed the need to continue this progress (European Commission, 2017). In 2015, the 'Riga Statement' emphasized the reinforcement of the counter-terrorism efforts on internal and external EU level and called on Europol to provide an improved environment for information exchange (Council of the European Union, 2015). This led to the 'Renewed Internal Security Strategy' of 2015, that highlighted the need for an effective response to terrorism through cross-border cooperation between the counter-terrorism units in the member states, supported by a pro-active central information hub at Europol (Council of the European Union, 2015). Further in 2016, the European Commission set up a 'High Level Expert Group' with the aim to address the current shortcomings and possible knowledge gaps concerning the used systems and its interoperability (European Union, 2016). To achieve finally an integrated information management system accessible for all competent authorities on EU level.

In 2013, the upcoming phenomenon of foreign terrorism fighters called the EU's attention back to the overarching topic of 'information management' and led to a deeper look on which tools and best practices have been served as worth for extension. In April 2016, the European Commission started the process of 'stronger and smarter information management systems', meaning that every competent authority receives the needed information systematically from

[18] The Prüm Decision is a multilateral treaty signed in 2005 between Germany, Spain, France, Luxembourg, The Netherlands, Austria and Belgium. The European Commission supported this initiative and adopted it in 2008 in the Council Decision 2008/615/JHA of 23 June 2008.

different information systems at their disposal (European Commission, 2016, p.3). Further in May 2016, under the Dutch European Council presidency, the EU CTC released a 'roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs Area' (Council of the European Union, May 2016). In this roadmap, the EU encouraged the use of Europol's capacities and capabilities to their maximum extent, aiming at the improvement of crucial information-sharing. A further formulated aim in this roadmap is to achieve a 'one-stop-shop information solution' at national and EU level, meaning to use a single-search interface system (Council of the European Union, May 2016). This in sum, shows only the recommendations by the political-administrative level, without taking into consideration the practitioner's needs. Deeming the developments so far, finally the EU CTC stressed in May 2016 the need to develop a 'practitioner-centred approach' which should include the ideas and recommendations by practitioners to arise with important points for further amendments. Having this in mind, this thesis is focusing on Europol to reveal the practitioner's views on the EU's information architecture, collecting the ideas by practitioners which could be the cornerstone for a 'practitioner-centred approach'.

3.2 Technical Capabilities of the IT-Systems

The aim of this paragraph is to provide an overview of the used systems in the EU and explain their capabilities regarding information exchange and ensuring at the same time counterchecks against the existing Europol databases. Within the European Institutions several tools have been provided by the European Commission, enabling especially law enforcement authorities to receive timely access to updated information and criminal intelligence to be able to predict, prevent and react on potential threats. The Schengen Information System (SIS) which is active since the late 1990s, is the most known information–sharing tool. It is most widely implemented compared to other IT-systems in the European Union and used by border police and law enforcement to consult alerts on missing or wanted persons and items. The SIS II experienced a reinvigoration in the wake of the foreign fighter phenomenon and terror attacks since 2013 (Vavoula, May 2016). Additionally, Europol supports the member states, serving as an information hub and providing a secure information exchange system with the Secure Information Exchange Network Application (SIENA). Europol can share information with law enforcement officers on specific cases with the member states but also with third countries under restricted conditions. Another instrument, offered by Europol for the member states, is the Europol Information System (EIS) which is the main database for the storage of information

within the Europol's mandate[19]. Other important networks which serve as information platforms are the European Platform for Experts (EPE), the Financial Intelligence Unit's network (FIU.net) to support the Financial Intelligence Units (FIUs) in the member states and the Passenger Name Records (PNR), [20]which is still under development in the member states, but also the Terrorist Finance Tracking Programme (TFTP)[21]. As well as the communication network of EU law enforcement authorities in the Police Working Group on Terrorism (PWGT)[22]. Even when these networks surely include the use of sophisticated IT-systems and therefore they have an added value for the exchange of information at large, they will be paid less attention in this thesis due to the lacking published knowledge on its IT-systems.

To sum up, the before-mentioned daily used IT-systems differ enormously in scope and functionality. Based on these conditions, the systems need to be geared to each other, whether by a technical upgrading or an improved interconnectivity. The aim is to use the most appropriate system for information exchange, ensuring a secure and necessary sharing of timely important and classified information which could become a new main pillar, serving as a functioning 'integrated information management system with a single search interface' in the EU (Council of the European Union, May 2016).

---

[19] Art. 3 of the Regulation (EU) 794 of 11 May 2016, starting to operate on 1 May 2017, describes Europol's mandate. Therefore, "[…] the objective of Europol shall be to support and strengthen action by the competent authorities of the member states and their mutual co-operations in preventing and combating serious crime affecting two or more Member States, terrorism and other forms of crime which affect a common interest covered by a Union policy, as listed in the annex." (Regulation (EU) 794, May 2016, Art.3).

[20] The PNR-directive was adopted in December 2015 by the European commission. The data can be used for prevention, investigation and detection of potential terrorists and serious organized crime (Council of the European Union, March 2016).

[21] The EU-US TFTP, which took effect on 1 August 2010, is based on an agreement between the European Union and the United States providing information and intelligence about international transactions to combat the financing of terrorism.

[22] It is planned to implement this communication network within the ECTC at Europol to ensure the full range of information exchange on counter-terrorism (Council of the European Union, May 2016, p.13).

3.2.1 Schengen Information System (SIS)

The Schengen Information System was established under the Schengen Agreement of 1986 and started to operate in 1995. It serves as a database with information in the form of 'alerts' about wanted persons and objects for criminal and policing purposes particularly used in offices at European Union borders (Dontu, 2014). The SIS has been substituted in 2013 by the SIS II, an upgraded version which is nowadays the most prevalent system in the European Union and has been regularly and lastly upgraded in early 2015, due to the upraising threats by terror attacks and the phenomenon of returning fighters from conflict zones outside the European Union. Its progress embraces the increase of offices with SIS-access, a facilitated information exchange on terrorist suspects as well as the capacity to invalidate travel documents from suspects with the purpose to travel to conflict zones. It is a sheer search system with hit/no hit notifications and the data input can be done in different 'categories' from law enforcement and border police, without providing a connection between the 'categories'. Indeed, this implies the restriction that a person or object need to be searched in the 'right category' for which the person is suspected. Regarding the search for potential terrorists nowadays, the EU CTC recommends the setting of the marker 'terrorism related activity', otherwise there cannot be generated a hit (Council of the European Union, May 2016). As opposed to this, in the case of a hit-notification, the provider of the originally information can be contacted for further information on that specific case. Furthermore, information about suspects can be added but merely in special implemented offices with SIS II-access, called SIRENE (Supplementary Information Requested at the National Entries). This service will be provided in the most member states by the ENUs[23], specific offices connected to Europol.

After 2014, the SIS II experienced a reinvigoration after several terror attacks occurred. Several times, the EU CTC addressed the need to use this tool for the registration of potential terrorists and foreign terrorist fighters. The increased data input leads to an increase of registered suspects in the last years. An upgrade of SIS II with new added categories are topics of the current proposals under discussion, for instance the storage of potential terrorists with the marker 'unknown wanted persons' and the full access rights for Europol (European Commission, March 2017).

[23] The European National Unit (ENU) is usually the federal police office on state level within the member states.

3.2.2 Europol Information System (EIS)

The EIS can be used by Europol itself and in more than 4.500 police offices in 28 member states. It serves as a database for storage and query of data on international organised crime and counter-terrorism (Europol-website, 2017). By the end of 2015, the EIS was already connected to 20 counter-terrorism units on EU level. Furthermore, this direct information system provides data on a suspect person, object or vehicle that can be washed against the existing databases (Analysis Work Files, AWFs) at Europol, resulting in an immediate reply whether any other European State has additional information on that suspect. The data in the EIS can be stored in different 'entities', to be individuals, vehicles, documents or objects and further these 'entities' can be connected to get a comprehensive picture of the case. Additionally, the EIS allows entering biometrics (DNA) for cross-checking and therefore, it has an overall advantage to other used systems within the EU as an information exchange system. To use these functionalities efficiently, the implementation of the so-called 'automatic data loaders' is in process, ensuring the automatic data transfer from the national systems to Europol (Council of the European Union, May 2016).

However, it should be emphasized that Europol's access to the most widely implemented system in the EU, the SIS II, is not entirely accessible for Europol staff. Its access is rather limited and no information can be added in the SIS II database by Europol staff or even extracted to store it in the EIS for further cross-checking (Council of the European Union, March 2016, p.14).

3.2.3 Secure Information Exchange Network Application (SIENA)

SIENA is a communication system that meets the requirements by law enforcement agencies. It ensures a secure and direct information exchange on crime related operational and strategic information with Europol, between the member states but also with third countries, depending whether they have a strategic or operational agreement (Europol-website, 2017). Since the EU CTC's efforts in April 2016, the SIENA system has been step by step expanded to intelligence services, in line with an upgrade of its safeguard level (Council of the European Union, March 2016). Within SIENA there has been established a dedicated area especially for counter-terrorism authorities, called SIENA CT with a direct connection to Europol. The SIENA CT is already operating with 95% in the member states, more precisely it offers a secure connection to 42 counter-terrorism authorities (Europol TE-SAT Report, 2016). By the end of 2016, SIENA ensures a classification level of 'confidential' compared to 'restricted' before, which was one of the main obstacles from intelligence services for its use (Council of the European Union, April 2016).

3.3 Current State of Play of Implementation Progress

In 2016, several implementation reports by the EU CTC have been launched to inform about the different initiatives and the progress that has been made. Concerning the SIS II, it can be reported an on-going progress. According to the EU-Lisa report 2016, the statistics show that the hits have grown up to 200.778 which is an increase of 30% compared to the year before in 2015, whereas round about 74% of these hits were triggered to alerts on persons (EU-Lisa, 2017). In addition, the plan to complement SIS II with a search function for fingerprints is in progress (Council of the European Union, December 2016). Furthermore, the rolling out of the SIENA CT-version shows progress. Whereas in the report from April 2016, the EU CTC still claimed that related to the feeding with names via SIENA CT of potential foreign terrorism fighters, 90% of the contributions by the member states merely originated from five member states, the awareness of the necessity to contribute to the ECTC at Europol will increase continuously by the end of 2017 (Council of the European Union, April 2016, European Commission, March 2017). Even when the EIS seems to be the most appropriate system for storage, cross-checking and exchange, the implementation of the 'automatic data loaders' in the member states are still under development.

3.4 Conclusion

It hardly can be argued, that the dragging process of implementation could be caused by a lack of initiatives and regulations. Quite the opposite, the Council of the European Union has taken widespread measures to tackle the identified shortcomings and fill the knowledge gaps. Further, the European Commission has provided Europol with the necessary tools to ensure an effective information exchange. Particularly, the implementation of the SIENA CT-version has contributed to more interconnectivity for the counter-terrorism units. However, the legal regulations for the implementation of IT-systems are still underlying the subsidiary principle of each member state and might be one reason for a delay of operating systems. Another reason could be the lack of capacity to process the masses of collected data. Furthermore, it should be stressed that beside all mentioned systems in this chapter, each member state works with its own national police IT-system, which are not automatically connected with the systems on EU level. Having this in mind, the discussion about the extension of the SIS II, as the one and only universal remedy on EU level, seems to be 'the scratching on the surface' and finally just a short-term solution. Moreover, in the sense of 'mind the gap', the information management architecture by the EU hampers due to its own complexity and therefore should be seen in different layers, on the one side what had already be done and on the other, what still needs to be done.

Concerning the role of the EU CTC, it is remarkable that especially during the Dutch Presidency, the reporting about the detailed implementation process was more regularly as ever before and insofar the role of the EU CTC could be described more active than before. As opposed to this, with the end of the presidency on 30 June 2016, the reporting almost fades away. Indeed, during the Dutch presidency the implementation process of EU's information systems accelerated evidently. Nonetheless, it could be argued that implementation progress can only be achieved if they are in line with the political interest by the European Council's presidency at that time. A claim that has been made several times before, identifying the shortcomings in the management and communication structures of the European Union.

4 Methodology

In this chapter I will set out the research design which is underlying this thesis. First, the choice of research type will be explained which will be followed by insights of the approach for the collection of data. Then there will be provided some information about the semi-structured face-to-face interviews with experts and the setting-up of an interview guide. Subsequently, the process of evaluation of the expert interviews and finally the limitations of this research will be explained.

4.1 Research Type

The research design adopted for this thesis is a *qualitative single case study*. A case study is the right choice to reveal the perspectives of practitioners in real life situations on concrete subjects. The definition for a case study that Yin (2003) used, is cited as follows "[…] a case study tries to illuminate a decision or a set of decisions: why they were taken and how they were implemented, and with what result" (Schramm, 1971, cited in Yin, 2003, p. 12). In addition, Yin (2003) states that a case study investigates a current phenomenon in a real-life context (p. 13). Reflecting to the research question, this thesis is focused specifically to evolve the practitioner's views on the EU's information architecture. Therefore, the unit of analysis are the tensions between the EU's policy and the practitioners and insofar the unit of observation will be Europol which is a central hub for information exchange. More precisely, the experiences and views by Europol's employees serve as a yardstick to better assess the tensions between the top-down and bottom-up perspectives. The aim is to get a deeper insight in the views, preferences and values of law enforcement practitioners regarding information architecture by the EU and further explain their alignment or non-alignment with the EU's policies.

The analysis in this research consists of two parts. The first part is focusing on a qualitative analysis of public available policy documents regarding the EU's efforts for an appropriate information management concerning the used IT-systems in the counter-terrorism domain. In relation to the research question, the second part is based on a case study to reveal the point of views by law enforcement officers about important themes (compared to concepts in quantitative research) around different areas of enquiry such as 'formal information exchange', 'main barrier trust', 'interoperability of used IT-systems' and the 'effectiveness of an integrated information management system'. Finally, with the aim to elucidate further *how* the above-

mentioned views by practitioners can be explained and whether we can identify a specific level of convergence in relation to the Europeanization process.

Concerning the themes, it should be taken into consideration that they are more subjective impressions and could vary in content from one respondent to another (Kumar, 2011). Even when the measurement of preferences and values seems to be difficult, Kumar (2011) states that it is indirectly possible by using appropriate indicators (p. 63). Because these views and preferences are based on reported behaviours in real life, the judgements that are followed by these 'behaviours' may differ from one person to another (Kumar, 2011). Therefore, the themes need to be converted into variables or better said, a set of indicators that can be measured, although the accuracy with which method they can be measured will probably differ from one individual method to another (Kumar, 2011).

In the end, both, the results from the analysis of the EU's information management in counter-terrorism and the views by practitioners will be critical analysed. Moreover, these fronting two 'visions or views' will be compared with the aim to work out the differences and similarities. Hopefully, the results can explain the dragging process of implementation in the field of counter-terrorism.

4.2 Data Collection Method

The process of data collection will be based on two data collection methods. Especially, data collection in qualitative research is considered to offer a high level of flexibility and freedom concerning the structure and order given to the researcher (Kumar, 2011). Thus, as a first step a desktop research has been done to build up the contextual framework, focussing on the measures derived from the European Union's information architecture. Second, face-to-face interviews complement the findings with experiences by hand selected practitioners working for Europol. Due to the fact, that the study has an explanatory (desktop research) as well as an exploratory (interviews) nature, the findings of the interviews need to be analysed in the light of the results from the before conducted desktop research, focusing on the views by the administrative-level of the EU.

The used data in this study is a combination of primary sources (policy documents, interviews, legislation etc.) and secondary sources (journal articles, news reports etc.). Generally speaking, Yin (2003) recommends three important principles that should be followed to ensure the quality of a case study: (1) multiple sources of evidence, at least two sources that can be converged on

the same set of findings, (2) a case study database, meaning the storage of evidence in a structured and orderly way, separately from the final case study report, and (3) a chain of evidence, more precisely the links between the given questions, the collected data and the conclusion must be ensured (p.83). Consequently, the collection of data with desktop research and face-to-face interviews is based on different sources to ensure a high quality of this study.

4.3 Semi-Structured Interviews with Experts

Naturally, data collection implies selection. Concerning the interviews, the sample for the study consists of six police officers employed by Europol and personally known to me. The police officers are carefully hand selected based on their current job duties and purposefully chosen to gain their views on real-life situations and experiences. Based on my own several years' experience as an analyst working in a security agency, I know that not every employee has the overview and foresight, nothing to say about the interest, regarding the political-administrative dynamics in their institution. Therefore, I selected just these ones who have a comprehensive overview about the developments in their home countries and can oversee the arising tensions at Europol. From my point of view, this is an indispensable precondition to ever recognize and assess these tensions between the political-administrative level and the practitioners.

Furthermore, Yin (2009) states that hand selected participants for interviews are crucial for case study designs to effectively achieve the aim of replication. Further, he argues that selecting the number of participants in a qualitative research is comparable to the number of experiments conducted in a quantitative study (Yin, 2003). The police officers have been contacted via email and depending on their schedule the duration and length for the interviews vary from one informant to another. In addition, the location has been chosen by the police officers themselves to guarantee an atmosphere that is convenient for the officers. Aside from that, the officers prefer to remain anonymous what is not unusual in interviews with law enforcement staff. However, for reasons of transparency and integrity, the names of the interviewees and the transcripts of the interviews have been provided to the supervisor of this thesis.

For this research, semi-structured interviews have been applied. According to Kumar (2011), an interview schedule is a research instrument for collecting data, a written list of questions prepared for use by an interviewer in a face-to-face interview (p.145). Admittedly, an interview schedule ensures on the one side a logical order of questions but on the other side it could limit the opportunity for the interviewee to come up with new raising issues that could serve as an added value for the study findings. With this said, an interview guide has been prepared as a

loose list of issues to leave room for unexpected issues mentioned by the interviewed practitioners (attached in the appendix 8.2). Not all questions will be asked because the practitioners are working in different units. To the contrary, the interviewees should have the freedom to talk about their point of views.

4.4 Evaluation of Expert Interviews – Coding

The interviews have been recorded and transcripts of the conducted interviews have been prepared for the coding and the analysis process. [24] The coding is in line with the themes upraised in the formulated research questions and the literature review, such as the 'formal information exchange', 'main barrier trust', 'interoperability of used IT-systems' and 'effectiveness of an integrated data management system'. In the operationalization scheme (attached in the appendix 8.1) several indicators have been worked out to be able to better validate the respective themes. This ensures a structured and conceivable explanation for the analysis process. Moreover, it guarantees that the findings of the research will be arranged according to the key elements of the main research question of this thesis.

4.5 Limitations

There are several limitations in a case study research. This qualitative case study reveals an insight in the perspective of Europol's employees which hardly can be compared to other types of research. And much less, the findings cannot be interpreted as 'the' view of Europol as an organisation. However, it reveals a hunch of practitioner's perspectives which are seldom and interesting itself. Furthermore, the use of a small number of participants in the interviews may compromise the ability to generalize the specific law enforcement-findings to other law enforcement organisations (Yin, 2003).

However, the purpose of the study was to get a deeper understanding of Europol's views towards the top-down driven information architecture by the EU. Deeming the results of the study, the real benefit of this case study is definitively to get the personal views from the practitioners dealing with the challenges on a daily-basis that could not be revealed with other

[24] The second interview have been undertaken in a different language than English. The author of this thesis is responsible for the translation into English (appendix 8.3.2.).

research types. Admittedly, even when it cannot be ruled out that the officers told the 'whole' truth, although it has been tried to mitigate this by offering anonymity.

Furthermore, it should be taken into consideration that all officers have prior professional experiences in their home countries. Therefore, they can provide an insight into the on-going implementation processes within their national law enforcement authorities. Although, this information is not within the focus of this research, it can however provide background information and therefore serve as an added value to understand better the different approaches in their countries based on prior experiences with terrorist attacks. Concerning the represented nationalities from Germany, France and Greece, it is noteworthy to mention that the countries have maybe, due to prior experience with terrorist attacks, a different view to the EU's top-down driven information architecture than other employees from other member states. Therefore, merely their view regarding the technical capabilities close related to the implementation process will be included in the analysis of this research.

Finally, this case study offers the opportunity to evolve with new ideas and recommendations better geared to the implementation process of EU's measures and to establish an added value for the academic literature in the field of governance of security at large.

5 Critical Analysis

In this chapter I will provide the two confronting 'visions' that have been revealed in this research. On the one side the political peculiarities which describe the logic of the political-administrative level of the EU and on the other side the empirical results explored by the interviews, representing the logic of the practitioner's level in law enforcement. The two 'visions' will be arranged according to the themes such as 'formal information exchange', the 'main barriers', interoperability of used IT-systems' and the 'effectiveness of an integrated information management system' as determined for this research. This will be followed by a critical assessment evolving the differences and similarities to be able to answer the underlying research questions in the following sixth and last chapter of this thesis.

5.1 Policy Peculiarities – Logic of Political-Administrative Level

The findings of the desktop research revealed the logic of the political-administrative level of the EU regarding its efforts on how to accelerate the implementation process towards the establishment of an 'integrated information management system in the field of counter-terrorism. Whereas since 2005, the European Union Counter Terrorism Strategy and the 'The Hague Programme' emphasized the first pillar, more precisely the 'prevention' of terrorism as a key task, the focus has been clearly shifted to the last pillar in the past years, namely the 'response' on terrorism. Meaning that also for the main actors such as the European Council on political level it became obvious to better align its efforts more to strengthen the solidarity in the EU, to advance the coordination of the response and to improve the capabilities to cope with terrorism. More precisely, to be more pro-active and perceptive on preventive measures.

Since 2013, the EU's efforts regarding the improvement of **formal information exchange** have experienced an extensive attention. Although, the need to simplify the sharing of information was already mentioned as an important topic in the European Council Framework Decision of 2006 (Council of the European Union, December 2006), little progress could be reported in that area in the following years. Initially in late 2013, with the uprising of the so-called phenomenon of foreign terrorist fighters in the EU, the pressing need for information exchange received a reinvigoration. In the Riga Joint Statement in 2015, the Council of Ministers of Justice and Home Affairs directly addressed Europol - for the first time in a long while - to build up the technical preconditions for a better information exchange environment and data-matching (Council of the European Union, February 2015). This was followed by the European Agenda

on Security of 2015 with specific formulated tasks or action plans that should guide the European Commission's work, monitoring the implementation process of these tasks. The developments in 2015 showed exemplarily, that the European Council had learned from prior experiences, meaning that it is not enough to simply mention the tasks in policy papers. Quite the opposite is the case, an implementation process needs to be monitored and checked on a regular basis (European Commission, April 2015). Further in this context, the more active role by the presidency of the EU Council should be paid more attention, particularly in the last two years. During the presidency of The Netherlands in the first half year of 2016, the focussing on topics such as the improvement of information-sharing in general accelerated enormously the process of implementation. Several implementation reports had been released with details about the state of play of the formal information exchange, encouraging to do further efforts. The responsible persons on political level identified the gaps, named the grievances and animated to keep track of the on-going actions. For instance, progressive steps such as the increasing number of listed potential foreign terrorist fighters in a database within the ECTC at Europol had been appreciated, whereas the insufficient use of these tools from merely five member states - state of play of October 2015 - had been criticized sharply (Council of the European Union, October 2015). As another example serves the repeating demand to further increase secondments of counter-terrorism staff and to contribute more to the EIS for cross-checking (Council of the European Union, March 2016, p.2). As opposed to this, the EU didn't foresee the challenges, popping up with the increased income of contributions and the collection of masses of data. Loosely based on the principle 'trust, but verify' the close collaboration and continuing efforts between the EU CTC and The Netherlands during its presidency caused an accelerated development and a visible progress in the field of information exchange, at least from the political top-level down to the European institutional level.

Regarding the **main barrier** for an effective information exchange, the political level merely named the barrier 'trust' and highlighted in this regard the necessity to use the provided operational services by Europol and other institutions on the EU level to the full extent. In addition, the EU recognized the human factor as an important and a crucial precondition for practitioners on national and EU level that needs to be taken into consideration (Council of the European Union, May 2016, p.7). However, even when the main barrier 'trust' has been mentioned several times in the policy papers, no recommendations have been forwarded to overcome this 'mistrust'. Moreover, neither mentioning possible trust-building measures have been made nor any ideas on how to fill the gap between intelligence services and law

enforcement agencies. With this said, the engagement by the political level to break down walls and build up trust is limited to a more patronizing advice to cooperate better among the member states and on European level. Moreover, the European Union did not address in any policy document the problem of its limited influence within the member states, obviously aware of its restricted powers as a supranational actor.

With a view to the efforts concerning a better **interoperability of the used IT-systems**, it can be stated that the EU paid much more attention on these topics. The EU reported about the current state of play of the new categories of the SIS II, the need to use the tools offered by Europol (EIS, SIENA, AWF, TFTP, PNR) to the maximum possible extent as well as reported about the progress on the rolling out of SIENA CT which connects increasingly the counter-terrorism units in the member states. In addition, the use of SIS II has been recommended specifically as a tool that can support investigations instead of merely using it limited as an instrument to support security checks (Council of the European Union, April 2016, p.6). Further, a closer cooperation between the member states and the Internet Referral Unit (IRU) at Europol has been recommended (Council of the European Union, April 2016, p.4). Another aspect that has been highlighted is the crime-terror nexus and the close related need to feed Europol with full data for data-matching (Council of the European Union, April 2016). With this said, the efforts concentrated already on newer and promising achievements in the counter-terrorism domain. Particularly, the forwarding of questionnaires to grasp the implementation status in the member states showed that the EU focused also on technical and practical issues and thereby it proves a strong actorness that finally can serve for more convergence of the acting agencies in the law enforcement and counter-terrorism domain.

With regards to the overall objective to establish an **effective 'integrated information management system'**, the EU has started an ambitious plan. Although, the European Council has recognized the high amount of used IT-systems on the EU level as well as in the member states and the enormous complexity of the information architecture in general, it has formulated an action plan to merge all tools in one system. More precisely, a system with only one single-search interface and an automated consultation-function of one system by another will be created (Council of the European Union, May 2016, p.3). One system for all practitioners on national and European level, which sounds on the one side promising but on the other side more than challenging. This plan has been presented as a major objective to be able to coordinate and store information to avoid that information can slip anymore through the cracks of security

services as happened in the past. This can be assessed as a real incentive task for the next coming years or decades. However, noteworthy in this regard is the already mentioned limited sphere of influence by the EU as a counter-terrorism actor, because the responsibility for any changes is still in the hand of the member states. Indeed, that could become a hampering effect against a full implementation of all measures. Conclusively, after a vast number of exhausting ambitions to improve the implementation process, the EU initiated in May 2016 a proposal to establish a practitioner-centred approach to better understand the requirements from these officers that are dealing with the problems on daily basis. This can be definitively assessed as a brave or wise step to evolve the concerns arising from the bottom (from the member states) instead of simply implementing them from the top (the political level), down to the European institutions without having any power to force the implementation process in the member states.

Although since 2013, the logic of the political-administrative level shows a higher attention for detail and for the needs of the practitioners on member states level than ever before, the released regulations still embrace merely the institutions and agencies in the sphere of influence of the EU policies. Even when questionnaires and surveys had been used to address the member state's problems on implementation, the dragging process of rolling-out the tools and the amount of actively participating member states in that process still shows a lack of interest for a closer cooperation. Therefore, the EU's logic can be described as simply still advisory and acting on uprising events due to its limited influence. As opposed to this, the increased efforts should be appreciated as well-structured and aim-oriented than ever before. Therefore, the logic of the political-administrative level so far contradicts the opinion in the academic literature, which described the EU's actions and motivations exclusively as patronizing (Bures, 2016, p. 61).

5.2 Empirical Results – Logic of Practitioner's Level

This paragraph aims to grasp the empirical reality of the conducted interviews. The findings revealed the logic of the practitioner's level and described the second 'vision', represented by employees at Europol. At the beginning of the interviews, I explained briefly my intention to conduct this research and presented an overview about the developments that are in progress on the political level. Further, I mentioned the efforts that have been done by the European Council to push the implementation process aiming at the following objectives: 1.) to improve the information exchange in general, 2.) to achieve a better interconnectivity of the used IT-systems on European level and 3.) to establish one system with a single-search interface with an automatically consultation from one system to another. Asked about their first impression and if they had known about these measures, all interviewees replied to know merely the efforts towards information exchange, but admitted nothing to know in detail about the plans on political level to establish one system for all purposes. The interviewees were from various centres hosted at Europol, such as two officers from the European Serious and Organised Crime Centre, one officer from the European Migrant Smuggling Centre, another officer from the European Counter Terrorism Centre and two officers from the Horizontal Operational Unit. All employees are dealing on daily basis with data concerning criminals that could be revealed as potential terrorists, based on the processing and cross-match capacities by Europol. However, most important is to grasp their view as practitioners about the EU's information architecture.

Concerning the **formal information exchange** in general, all interviewees confirmed that the information exchange between the member states and Europol has been improved and numerically increased in the last years, caused by the incoming contributions from the member states. Further, all respondents identified information exchange as crucial and important to detect potential terrorists and uprising trends that could be of significance for the security of the European Union. Particularly with a focus on formal information exchange, all interviewees emphasized the precondition to avoid anonymous contact addresses, such as post-offices, and underlined the need of personal contacts for an effective information exchange via the secure channels (SIENA). Additionally, it has been stated that the IT-systems serve simply as 'facilitators' because the human factor should not be unnoticed (interview 3). The professional analysis skills and experiences of practitioners are inevitable to judge about the importance of the information or intelligence to be able to decide what information could be useful in further investigations (interview 3). This affects the capacity to distinguish between information simply provided by a source or intelligence that is already assessed information by a law enforcement

authority (interview 3). In the following steps of an investigation the ability to prioritise has been described as vital to decide" […] how to know, who should know it" (interview 5). Whereas all interviewees assessed the information exchange in their daily work as well working, insights about the conditions in the member states had drawn another picture. For instance, one of the interviewees reported of enormous administrative barriers in one of the migration hot-spots[25] supported by Europol and described them as "[…] a mile to go to get the information to Europol" (interview 4). A vast number of units in the hierarchy must be contacted before one central unit appraises about and approves the transmission of the information, a very time-consuming but surely usual proceeding like in other countries (interview 4).

Regarding the information exchange's state of play between law enforcement and intelligence services, no one of the interviewees could give illuminating information providing a comprehensive picture of the cooperation. Merely the interviewee from the ECTC confirmed an existing cooperation but without giving further details (interview 5). All others negated any cooperation at least for their units. Based on the interviews it can be inferred that obviously within the building of Europol, there still exist a strict separation between the ECTC and the rest of Europol employees which can hardly assessed as beneficial for cooperation. One of the interviewee confirmed, based on prior professional experience, that intelligence services and law enforcement agencies have different cultures in their approaches and the protection of the source and information, even when both are pure security services (interview 3). Another interviewee assumed the cooperation in counter-terrorism matters as 'few decades behind' and compared the current stage of 'cautious convergence' with the situation in the serious and organised crime domain several years ago. He emphasised the common awareness as crucial to understand that cross-border terrorism cannot be investigated anymore from a national perspective (interview 1). There needs to be a common interest for a common response, that is at least the cognition based on suffered terror attacks in their home countries (interviews 1 and 3). Further, it has been stated that often the cooperation is hampered due to the pretext of secrecy, but based on experiences on national level, often it's just caused by the lack of willing to share information (interview 3). As a recommendation for an effective information exchange and particularly the first approach to get in contact, the operational meetings had been mentioned as a promising experience. Once this meetings on working level had been taken place, the sharing of information works much more smoothly to find common solutions for the

[25] Europol supports migration hot-spots in Italy and Greece with investigators if required.

investigations (interview 3 and 6). Further, the arrangement of workshops between practitioners and representatives of the political level to share 'best practices' but also 'bad practices' served as useful tools to enhance the cooperation (interview 3). These meetings have been proven to be the best opportunity to develop and exchange 'what is working, what is not working' (interview 3). All interviewees appreciated the services provided by Europol and assessed its analytical capacities as the state of the art of modern analysis applying innovative methods. Further, all respondents mentioned the added value of Europol as a big chance for the member states to be able to receive a comprehensive picture of the threats facing the European Union, instead of merely trust on bilateral exchange which can in worst case lead to a 'linkage blindness' (interview 3). [26]

Questioned to their opinion to the **main barriers** that could hamper an effective information exchange, three participants named immediately 'trust' as an important precondition (interview 1, 3,4). Whereas, all respondents mentioned the inevitable need for personal contacts, building through informal information exchange the groundwork for a following easier sharing of information via formal channels. A common agreement could also be reached on the operational meetings as a trust-building measure. Once the investigators in the member states have requested operational support from Europol - provided that the case fits in Europol's mandate - an operational meeting will be planned as the first approach to get together all the investigators that are dealing with this case. The experience of this first stage of information exchange and get to know to each other, often served as an opportunity to appreciate Europol's added value that can facilitate further cooperation (interviews 1, 3 and 6). Another barrier that has been mentioned already in the overall review to the 'formal information exchange' of this paragraph, is the 'reluctance' to share information with anonymous contact points and without knowing for which purpose. Meaning who will use the information, what will be done with it and will it probably forwarded (interviews 1, 3, 4, 6)? Subsequently, the interviewees named the 'language barrier' as a in part still remaining obstacle that merely can be solved in the member states with language training for the law enforcement officers to enable them to write requests in English and thereby feel more confident to communicate on international level (interviews 1, 4, 6).

[26] The term 'linkage blindness' is used in criminology and describes the situation when police departments do not communicate with each other and therefore they have no means of knowing that similar crimes have been committed in different geographic areas (Gainess L.K. et al, 2007, p.59).

The increase of information exchange in general is closely related to an unavoidable **collection of masses of data.** This has been stated by all participants as a success story, because Europol serves as the European Union's law enforcement criminal information hub and the advertisements by Europol obviously find in the member states approval. Further, it has been stated that there is a need of a crucial mass of data to find overlaps and to get a comprehensive picture of certain crime patterns but also future crime trends. Admittedly, several interviewees complained about the huge amount of data which needs to be processed which is very time-consuming (interviews 1,4,6). Supplementary, the workload caused by the backlog[27] reduces time that could be used for criminal analysis reports and projects (interviews 1, 4, 6).
As opposed to this, all interviewees agreed that the member states should be instructed to send data of a higher quality than simply more data. Indeed, in this context there has already began a change of paradigm and moreover, Europol has started to increase the recruitment for additional operational analysts, enhancing its analysis capacities (interviews 2 and 6).

With a view to the **interoperability of the used IT-systems**, the interviewees are mainly satisfied with their tools and recognise several changes and the ongoing implementation process to link, advance and adjust the different IT-systems. They also agree with their access to the most important IT-systems relevant to fulfil the main duties. Whereas only a few access-points to the SIS II exist at Europol, all respondents would appreciate the use of it. The increased data input in the SIS II during the huge influx of refugees to the European Union in 2015[28], could be of interest in some cases but, the checks in this system are for Europol analysts not obligatory (interviews 1 and 4). The SIS II is more used for search actions in the field of border management and this purpose is not covered by Europol's mandate[29]. Nevertheless, the most

[27] The term 'backlog' is used by practitioners at Europol to describe the accumulation of still unprocessed requests contributed by the member states.

[28] It has been stated in an implementation report by the Council of the European Union, that "[…] it is not possible to distinguish how many alerts concern FTF/terrorists. FTF/terrorists may also appear under other alert categories such as alerts for arrest or refusal of entry. Difficulties include: the compatibility rules between alerts, which hinder the creation of alerts under different articles for the same person (e.g. Art. 26 SIS II (in case a European Arrest Warrant has been issued for a FTF) and Art. 36 SIS II)" (Council of the European Union, March 2016).

[29] According to Europol's mandate, "[…] the objective of Europol shall be to support and strengthen action by the competent authorities of the member states and their mutual co-operations in preventing and combating serious

used systems show advantages as well as disadvantages that delay sometimes the procedures. The transmission system SIENA, for instance, still has a limited community caused by the restricted access and not yet finalised implementation process in the member states. Further, the transmissions are sometimes too slow that practitioners prefer the universal use of email with personal contacts and not anonymous contact offices such in SIENA (interview 2). Nonetheless, the use of SIENA for official requests is inevitable and obligatory to start action, highlighted by every employee in the interviews. All interviewees appreciate the efforts related to the increase of numbers of access to the EIS because they appraise it as a useful system and highly relevant on international level. It has the most widespread changes related to the implementation of digital interfaces that are provided by Europol to the member states, allowing an automated upload of national data to Europol (interview 2). Supplementary, some interviewed persons assessed the AWFs as an ideal database to store also soft data and background information, helpful to build a comprehensive picture of the crime fields and mobile organised crime groups (interviews 1 and 2). However, noteworthy in this regard is the indication by the respondents that despite of several used systems on European level, every member state uses its own national IT-system, often insufficient connected to the European systems. Further, they highlighted the need for a wise coordination due to the complexity of IT-systems on European level (interviews 1, 2,4).

In relation to an **effective integrated information management system**, the participants were requested to state their opinion to it in the last stage of the interviews. In a first step, they were asked about their opinion to the plans to establish a system with a single-search interface for all purposes, as described in the introduction of the interviews. As expected, all respondents were delighted of the imagination of a user-friendly system that can be used by all officers and everywhere. Some called it ‘great’ and others ‘utopia’. But shortly after their first reaction they raised objections regarding the complexity of the IT-system’s landscape. They assumed that the timeframe of approximately a decade can be expected until it will be available, nothing to mention the skyrocketing costs for the implementation (interviews 3, 4, 6). Further, the member state’s own IT-landscape needs to be taken into consideration as well as the difficulty to coordinate everything under the current national legal aspects and data protection rights, what has been assessed as difficult enough in smaller groups instead of coordinating it with 28

crime affecting two or more Member States, terrorism and other forms of crime which affect a common interest covered by a Union policy, as listed in the annex” (Regulation (EU) 794, May 2016, Art.3).

member states (interview 2). However, the solution based on a single system lets fondly hope to have finally more time for the setting up of important analysis reports than to simply processing data (interview 4).

In a second step the interviewees were bidden to describe their own imagination and thoughts of an 'effective integrated information management system' within the European Union for counter-terrorism purposes. Whereas almost all appreciated the efforts of the last years and identified them to be on the right way in the right direction, some mentioned as added value the extension of the IT-systems as crucial. Such as the rolling-out of SIENA CT or Europol's provision of a digital interface for the EIS connecting it to the member states (interviews 2 and 6). Others emphasized the need raising the analytical skills on national level in the member states to be able to decide about the 'right' data before it will be transmitted to Europol (interviews 3, 4). Finally, one interviewee came up with a very crucial recommendation, the respondent advised to agree in a first step on a common format on how specific entities should be stored such as name, surname, date of birth and so forth (interview 4). This has been highlighted as essential, building up the groundwork for the responsible dealing with sensitive and classified data.

Concerning the **EU's actorness in the counter-terrorism domain**, all interviewees mentioned within the discussions the limited influence by the European Union due to the still existing sovereignty of the member states. All released measures find their way from top-down to the European institutions, including Europol, but to decide about a further implementation within the landscape of the member states, the EU's hands are tied. Whereas several participants talked in the interviews also on their experiences from prior posts on national level, they portray the IT-landscape as widely complex and even difficult to coordinate innovations on national level (interview 3). Nothing to say about the difficulties to implement a common system in the countries with a federal structure like in Germany for instance, where every federal state runs its own databases (interviews 1, 2 and 4). In the light of these remarks, it appears as necessary that even for a recommended improvement of analytical skills on national level, more efforts and participation by the member states on the restructuring of the EU's information architecture needs to be targeted.

5.3 Critical Assessment regarding Similarities and Differences

Both 'visions', the political peculiarities as well as the empirical results by the interviews serve as the basis to develop an assumption about the similarities and differences of the two perspectives. At the first sight, the two visions seem to have the same opinion about what needs to be approached to achieve a considerable advancement of the current information architecture. Indeed, in all determined themes which are underlying this research, similarities can be found concerning the formulated targets. With this said, both sides name the extension of the sharing of information via the secure channels as the most important aim. This applies further for the main barrier of 'trust', identified on the political but also on the practitioner's level as the main obstacle. A further closer convergence can be seen in their motivations and steps towards the rolling-out of the mainly used IT-systems, proven to be successful. Finally, the two groups have a similar illusion of one system that can be used by everyone and for all purposes with automatic uploading functions and regular cross-checking mechanism. To sum up, merely the formulated targets prove to be a similarity in both levels.

Deeming the differences, it should be remarked the two different fields of professional operations with seldom opportunities of personal contacts with each other, manifesting the huge gap between the two 'worlds'. During their attempts to tackle a vitalised formal information exchange, the institutional players on political level are entirely limited to give advice and formulate hopefully initial and connecting factors. They merely can influence passive the process. Unlike the practitioners, who have the full range of possibilities to initiate actively a more frequented formal information exchange. Their incentives can build up trust which has been identified by both sides to be imperative for a longstanding cooperation with 'tools' such as operational meetings, awareness-rising events or simply personal communication. By contrast, the players on the political level can merely name trust as important, what they did in several policy papers, too. Nevertheless, their active role in this process is more than limited. Differences can further be identified in their actorness concerning an improved interoperability of the used IT-systems. In this field, the political level has an advantage over the practitioners. Whereas, the political-administrative actors can push the developments due to their comprehensive overview about the IT-landscape in the member states, on EU level and their financial resources, the practitioners can only work with the equipment that the policy provides at their disposal. However, one of a major shining out difference is their behaviour towards the member state's sovereignty. Whereas, almost all practitioners in this study addressed the reluctant or in part blocking actorness by the member states against the renewing of the EU's information architecture, this issue has been blinded out in the most policy papers on political

level. Inherently, there is just mentioned the kind advice to take more action in the overall process of a new information management system.

6 Conclusion and further Approaches

This thesis has elucidated the law enforcement's perspectives on the EU's efforts to establish an 'integrated information management system' for counter-terrorism purposes. In this respect, the main research question for this thesis is '*How do law enforcement practitioner's views align with or differ from the top-down driven information architecture by the European Union and how can this be explained?*' The Council of the European Union has increasingly pushed the implementation process for an improved information architecture in the last years. Based on interviews with employees from Europol, the research explored that in large parts the practitioners align with the formulated targets aiming at the establishment of an integrated data management system. They appreciate any improvement that could help to detect potential terrorists earlier and solve crime more effectively. Additionally, their alignment can be explained with the possibilities to advance the information exchange which are lying in the responsibility of themselves, they can in fact follow a more intensive sharing of information. Even when the practitioners assess the EU's plans as self-confident and ambitious, doubts have been claimed concerning boundaries of implementation outside the sphere of the EU's influence, respectively within the member states. The EU is reduced in its actorness and cannot oblige the member states to serve for more cohesion on EU level.

Concerning an effective information management, the practitioners appreciate the broader implementation based on the extension of the IT-systems right up to decentralized areas in the member states. This should be combined with the increase of analytical skills on national law enforcement level, to be better able to distinguish between highly qualitative and useless intelligence but as well about the appropriate amount that should be transmitted, avoiding an overload with masses of data. As primary barriers, the practitioners mentioned beside 'the lack of trust' also 'anonymity' and the 'language' as possible obstacles that hamper the progress. Thus, the practitioner's views differ from the policy's perspective insofar that the policy documents are entirely aim-oriented and focused on solving the reluctance and the ponderousness in the member states. However, the aim on political-administrative level is to build up the technical and methodical preconditions to establish an environment for information exchange. Hopefully to motivate the practitioners to apply and use their services. Subsequently, the interviewees named some promising recommendations such as the setting up of operational meetings to establish personal contacts, exchange best practices and find common solutions. Further, workshops in small groups with mixed participants from different investigative levels have been recommended. As the most banal suggestion, but probably the most essential one, is to first agree on a common format how to store basic information in the lowest levels of law

enforcement hierarchy in national databases to facilitate the workflow of information. The fact that these kinds of thoughts are in discussion, let simply guess what 'messy order or orderly mess' exists in the IT-system landscape of the EU.

Reflecting the body of knowledge in this thesis, it can be assumed that the analysis of a 'gap' between the political-administrative level and the practitioner's level is merely in part true. The efforts by the European Council to push the implementation process have surely contributed to a step-by-step improvement, even when slowly. Further, they could not withstand the 'seduction' of drafting repeatedly new blue-prints from above. However, the efforts during the presidency of The Netherlands could clearly accelerate the developments towards convergence due to their focus on trust-building and the 'practitioners-centred approaches'. This idea of an approach came up in May 2016 after several setbacks of the implementation process took place. The empirical results of this study, even when limited in the extent of participants in the interviews, can serve as a first tiny 'practitioner-centred approach', filling a gap in the academic literature. Then subsequently, this can be recommended for further academic approaches. The academics should acknowledge that the situation is changing, even when slowly. Therefore, we should keep also the small steps under review to be able to adapt them to the academic knowledge. With this said, further research on these topics are highly recommended. For instance, to explore the current state of play of implementation within the member states. Surely, this ambitious approach would require the revealing of the situation in all member states to get a comprehensive picture as well as to ensure a comparison of the respective member states in a later stage.

Deeming the academic body of knowledge, it can be stated that most of the literature is focusing on European level or on national level but seldom on interrelations between them. Based on the findings of this research, studies that combine these two perspectives would be an added value for the academic body of knowledge. The practitioners often name the plans by the EU 'to be out of touch with reality' because they know based on practical experiences the difficulties to align with all those systems, the different cultures and beliefs. Academic studies that include both views could reduce reservations.

The long-standing and widely held view in the academic literature that 'the lack of trust' is the main barrier for cooperation (Walsh, 2006; Müller-Wille, 2008), still can be confirmed in this research. In addition, the statement that it is important to know for the practitioners 'for which purpose the data will be exchanged' (Paulussen, 2016), is still identified as an important issue.

However, the practitioners at Europol have been more innovative in their efforts to more information- sharing, maybe due to fact that Europol is a ‘flagship’ for analysis and serves as the EU’s criminal information hub.

Conclusively, the results of the thesis show that the gap between both groups is getting closer, even step-by-step. Although, the politicians and police officers concentrate mostly on their own field of work, the awareness is rising that the two fields influence each other. Thus, the main challenge still is to elucidate on how the recommendations by practitioners can be adapted on political level. Deeming the suggestions of the study, workshops consisting of experienced practitioners and representatives of the European Council, both provided with full powers, could serve as the way forward. This should be the focus for the foreseeable future, a closer cooperation between security services, the policy and the academics for a common powerful response on terrorism in the EU.

7 Bibliography

7.1 Books, Articles and Journals

- Aalberts, T. E. (2005), 'Sovereignty Reloaded? A Constructivist Perspective on European Research', ConWEB, No. 2, retrieved from https://www.wiso.uni-hamburg.de/fileadmin/sowi/politik/governance/ConWeb_Papers/conweb2-2005.pdf.
- Argomaniz, J. (2010) 'Post-9/11 institutionalization of European Union Counter-terrorism: Emergence, Acceleration and Inertia' School of Politics and International Relations, University of Nottingham, pp. 1 -29.
- Argomaniz, J., O. Bures & C. Kaunert (2015) 'A Decade of EU Counter-Terrorism and Intelligence: A Critical Assessment, Intelligence and National Security', 30:2-3, 191-206.
- Bakker, E. (2006) 'Differences in Terrorist Threat Perceptions in Europe, in D. Mahncke and J. Monar (eds.) *International Terrorism. A European Response to a Global Threat?* (Brussels: P.I.E Peter Lang).
- Börzel, T. A., (2002), 'Pace-Setting, Foot-Dragging, and Fence-Sitting: Member State Responses to Europeanization.' Journal of Common Market Studies, Vol.40, No. 2, pp. 193 – 214.
- Börzel, T.A. & Risse (2003), 'When Europe hits … beyond its borders: Europeanization and the near abroad', Berlin Center for European Studies, published in Comparative European Politics, Volume 9, 4/5, pp. 394 – 413.
- Bossong R. (2013) EU cooperation on terrorism prevention and violent radicalization: 'Frustrated ambitions or new forms of EU security governance?', Cambridge Review of International Affairs, 27:1, 66-82,
- Bures, O. (2016) 'Intelligence sharing and the fight against terrorism in the EU: Lessons learned from Europol, European View, Volume 15, pp. 57 – 66.
- Brown, D. (2010) 'The European Union, Counter Terrorism and Police Cooperation, 1992 – 2007. Unsteady Foundations?, A question of credibility: Information Exchange. Oxford University Press, Chapter 6, pp. 147 – 190.
- Den Boer, M. & Van Buuren, J. (2012), 'SECURITY CLOUDS - Towards an ethical governance of surveillance in Europe', Journal of Cultural Economy, Vol. 5, No. 1, pp. 85 – 103.
- Den Boer, M. (2015) 'Counter-Terrorism, Security and Intelligence in the EU: Governance Challenges for Collection, Exchange and Analysis', Intelligence and

National Security, 30:2-3, pp. 402 – 419.

- Den Boer M. & Wiegand I. (2015) From Convergence to Deep Integration: Evaluating the Impact of EU Counter-Terrorism Strategies on Domestic Arenas, Intelligence and National Security, 30:2-3, 377-401, DOI: 10.1080/02684527.2014.988450.
- Den Boer, M. (2015), 'Counter-Terrorism, Security and Intelligence in the EU: Governance Challenges for Collection, Exchange and Analysis', Intelligence and National Security, 30:2-3, pp. 402 – 419. DOI: 10.1080/02684527.2014.988444.
- Ferreira-Pereira, L.C., Oliviera Martins, B. (2014) 'The European Union's Fight Against Terrorism: The CFSP and Beyond'. Shaffer, Ryan.
- Gaines L. K. & Miller R. L., 2007, 'Criminal Justice in Action', Thomson Wadsworth, Belmont, USA, Chapter 2, pp. 32 – 64.
- Giumelli F. (2012) 'Oldrich Bures. EU Counterterrorism: A Paper Tiger?', Terrorism and Political Violence, 24:3, pp. 520-522, DOI: 10.1080/09546553.2012.684614.
- Kaunert, C. (2010) 'Europol and EU Counterterrorism: International Security Actorness in the External Dimension, Studies in Conflict & Terrorism, 33:7, pp. 652 – 671, DOI: 10.1080/1057610X.2010.484041.
- Knill, C. (2005) 'Introduction: Cross-national policy convergence: concepts, approaches and explanatory factors', Journal of European Public Policy, 12:5, 764-774, DOI: 10.1080/13501760500161332.
- Kumar, R. (2011) 'Research Methodology', 3rd Edition, Sage Publications.
- Lawrence Neuman, W. (2014), 'Social Research Methods: Qualitative and Quantitative Approaches', Seventh Edition, Chapter 6 and 14, pp. 165 – 210 and pp. 477 - 513.
- Monar, J. (2015) 'The EU as an International Counter-terrorism Actor: Progress and Constraints, Intelligence and National Security', Vol. 30, No.2-3, pp.333-356.
- Müller-Wille, B. (2008) 'The Effect of International Terrorism on EU Intelligence Cooperation', Journal of Common Market Studies, Volume 46, Number 1, pp. 49-73.
- Radaelli, C. M. (2003), 'The Europeanization of Public Policy', pp. 27 – 56.
- Schroeder, U.C. (2009) 'Strategy by Stealth? The Development by EU Internal and External Security Strategies', Perspectives on European Politics and Society, Volume 10, No. 4, 486 – 505.
- Swanborn, P. (2010) 'Case Study Research: What, Why and How?', First Edition, Sage Publications.
- Walsh, J. (2006) 'Intelligence-Sharing in the European Union: Institutions Are Not Enough', Journal of Common Market Studies, Volume 44, Number 3, pp. 625 – 643.

- Walsh, J., L. Tushman, J. Kimberly, B. Starbuck, S. Ashford (2007), 'On the Relationship Between Research and Practice – Debate and Reflections', Journal of Management Inquiry, Vol. 16 No. 2, pp. 128 – 154.
- Yin, R. K. (2003) 'Case Study Research, Design and Methods', Volume 5, 3. Edition, Sage Publications.
- Yin, R. K. (2009) 'Case Study Research, Design and Methods', Volume 5, 4. Edition, Sage Publications.

7.2 Policy Documents

- Council of the European Union (2001) Anti-terrorist Roadmap, SN 4019/01, 26 September 2001.
- Council of the European Union, 2002, 'Council Framework Decision of 13 June 2002 on combating terrorism', 2002/475/JHA, Brussels.
- Council of the European Union, 2005, 'The Hague Programme: Strengthening Freedom, Security and Justice in the European Union', Official Journal of the European Union, 2005/C53/01, Brussels.
- Council of the European Union, 2005, 'The European Union Counter-Terrorism Strategy', 14469/4/05 REV 4, 30 November 2005, Brussels.
- Council of the European Union, 2006, 'on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union', 18 December 2006, Official Journal of the European Union, 2006/960/JHA, Brussels.
- Council of the European Union, 2008, 'Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, 23 June 2008, Official Journal of the European Union, 2008/615/JHA, Brussels.
- Council of the European Union, 2008, 'Council Framework Decision 2008/919/JHA of 28 November, 2008 amending Framework Decision 2002/475/JHA on combating terrorism', 2008/919/JHA, Brussels.
- Council of the European Union, 2009, 'Council Decision of 6 April 2009 establishing the European Police Office (Europol), 6 April 2009, Official Journal of the European Union, 2009/371/JHA, Brussels.
- Council of the European Union, 2010, 'The Stockholm Programme – An Open and Secure Europe Serving and Protecting the Citizens', Official Journal of the European

Union, 2010/C115/01, Brussels.

- Council of the European Union, 2015, 'Riga Joint Statement – Informal Meeting of Justice and Home Affairs Ministers in Riga on 29 and 30 January 2015', 2 February 2015, 5855/15, Brussels.
- European Commission, 2015, 'The European Agenda on Security', 28 April 2015, COM(2015) 185 final, Strasbourg.
- Council of the European Union, 2015, 'Draft Council Conclusions on the Renewed European Union Internal Security Strategy 2015 - 2020', 10 June 2015, 9798/15, Brussels.
- Council of the European Union, 2015, 'Follow-up to the statement of the Members of the European Council of 12 February 2015 on counter-terrorism: State of play on implementation of measures', 5 October 2015, 12318/15, Brussels.
- Council of the European Union, 2015, 'Fight against Terrorism: implementation of short-term actions', 5 October 2015, 12551/15, Brussels.
- Council of the European Union, 2016, Meeting report, 'State of play on implementation of the statement of the Members of the European Council of 12 February 2015, the JHA Council Conclusions of 20 November 2015, and the Conclusions of the European Council of 18 December 2015, 4 March 2016, 6785/16, Brussels.
- Council of the European Union, 2016, Meeting report, 'Systematic feeding and consistent use of European and international Databases – information sharing in the counter-terrorism context', 14 April 2016, 7726/16 Brussels.
- Council of the European Union, 2016, Meeting report, 'Draft Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area', 13 May 2016, 8437/16, Brussels.
- Council of the European Union, 2016, Meeting report, 'Information sharing in the counter-terrorism context: Use of Europol and Eurojust', 31 May 2016, 9201/16, Brussels.
- Council of the European Union, 2016, 'Implementation of the counter-terrorism agenda set by the European Council', 20 December 2016, 14260/16 Brussels.
- European Commission, 2016, 'REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision

2010/261/EU', Official Journal of the European Union, 21 December 2016, 2016/C257/03, Brussels.

- European Union High Representative for the CFSP, 2007, 'Javier Solana, EU High Representative for the CFSP, appoints Mr Gilles de Kerchove as EU Counter-Terrorism Coordinator', 19 September 2007, S256/07.
- European Commission, 2016, 'Setting up the High -Level Expert Group on Information Systems and Interoperability', Official Journal of the European Union, 17 June 2016, 2016/C257/03, Brussels.
- European Commission, 2017, 'Report from the Commission to the European Parliament, The European Council and the Council – Fifth progress report towards an effective and genuine Security Union', 2 March 2017, COM(2017) 203 final, Brussels.
- Regulation (EU) 2016/794 of the European Parliament and the European Council, 2016, 'on the European Union Agency for Law Enforcement Cooperation (Europol) and the replacing and repealing Council Decision 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA', 11 May 2016, Official Journal of the European Union, Brussels.

7.3 Online Sources

- Bigo D. et al. (April 6, 2016), 'The EU and the 2016 Terrorist Attacks in Brussels: Better instead of more exchange', Center for European Policy Studies, retrieved from https://www.ceps.eu/publications/eu-and-2016-brussels-terrorist-attacks-better-instead-more-information-sharing
- Bunyan, T. (1993) 'Trevi, Europol and the European State', Statewatch, retrieved from http://www.statewatch.org/news/handbook-trevi.pdf
- CEPS Thinking ahead for Europe, 2016, 'The EU and the Terrorist Attacks in Brussels: Better instead of more information sharing', 6 April 2016, Brussels, retrieved from https://www.ceps.eu/content/about-ceps
- De Kerchove, G. (30 September 2016), Speech by Gilles De Kerchove, EU Counter-Terrorism Coordinator: "Jihadi attacks reveal EU failures of imagination", retrieved from https://understandingjihadismterrorism.wordpress.com/2016/12/12/gilles-de-kerchove-eu-counter-terrorism-coordinator-jihadi-attacks-reveal-eu-failure-of-imagination/

- Deutsche Welle (2017, January 18), 'Anis Amri: How a terror suspect eluded German authorities' retrieved from http://www.dw.com/en/anis-amri-how-a-terror-suspect-eluded-german-authorities/a-37180968
- Dontu M., 'Schengen Information System', 18 September 2014, retrieved from http://dx.doi.org/10.2139/ssrn.2498006
- EUR – Lex, Access to European Union Law, 'Treaty on the European Union', retrieved from http://eur-lex.europa.eu/summary/chapter/justice_freedom_security.html?root_default=SUM_1_CODED%3D23,SUM_2_CODED%3D2307&locale=en
- European Commission, MEMO Brussels, 'Special Eurobarometer Survey: European's Attitudes Towards Security', April 2015, retrieved from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/20150408_1_memo_eurobarometer_april_2015_v2_en.pdf
- European Commission – Migration and Home Affairs, 'Information exchange', retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange_en
- Europol, 'Europol Information System', 26 April 2017, retrieved from https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system
- Europol, 'Information Exchange', 26 April 2017, retrieved from https://www.europol.europa.eu/activities-services/services-support
- Europol, 'European Union Terrorism Situation and Trend Report 2016', 2016, retrieved from https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report
- EU-Lisa, 'SIS II 2016 Statistics', April 2017, retrieved from http://www.eulisa.europa.eu/Publications/Reports/SIS%20II%20-%20Statistics%202016%20-%20factsheet.pdf
- ICCT, 'The Foreign Fighters Phenomenon within the European Union', April 2016, retrieved from https://www.icct.nl/wp-content/uploads/2016/03/ICCT-Report_Foreign-Fighters-Phenomenon-in-the-EU_1-April-2016_including-AnnexesLinks.pdf
- National Strategy for Information Sharing – Successes and Challenges in Improving Terrorism-related Information Sharing (October 2007), retrieved from https://nsi.ncirc.gov/documents/National_Strategy_for_Information_Sharing.pdf

- Nelson, R. (2011) 'Information-Sharing in Security and Counterterrorism – The challenge of Balancing Sharing with Security', Centre for Strategic and International Studies, retrieved from https://www.csis.org/analysis/information-sharing-security-and-counterterrorism
- Nelson, R. (2011) 'Information-Sharing in Security and Counterterrorism – The challenge of Balancing Sharing with Security', Centre for Strategic and International Studies, retrieved from https://www.csis.org/analysis/information-sharing-security-and-counterterrorism

  Paulussen, C., (2016) 'Repressing Foreign Fighters Phenomenon in Western Europe: Towards an Effective Response Based on `Human Rights, ICCT International Centre for Counter-Terrorism -The Hague, ICCT Research Paper, November 2016, retrieved from https://icct.nl/wp-content/uploads/2016/11/ICCT-Paulussen-Rule-of-Law-Nov2016-1.pdf
- Radaelli, C. M. (2000), 'Whither Europeanization? Concept Stretching and Substantive Change', European Integration online Papers 4(8), retrieved from http://eiop.or.at/eiop/texte/2000-008.htm.
- The Guardian, 1 June 2014, 'French suspect in Brussels Jewish museum attack spent year in Syria', retrieved from https://www.theguardian.com/world/2014/jun/01/french-suspect-brussels-jewish-museum-attack-syria
- Travis, J. (1998) 'Informal Information Exchange Among Police Agencies', National Criminal Justice Reference Service, retrieved from https://www.ncjrs.gov/pdffiles/fs000233.pdf
- Vavoula N., 'Detecting foreign fighters: the reinvigoration of the Schengen Information System in the wake of the terrorist attacks', 3 May 2016, Queen Mary University of London, retrieved from http://eumigrationlawblog.eu/detecting-foreign-fighters-the-reinvigoration-of-the-schengen-information-system-in-the-wake-of-terrorist-attacks/

8 Appendix

8.1 Operationalization scheme

Themes	Indicators
'formal information exchange'	• Interconnectivity of used IT-systems at Europol • Degree of interoperability with member states • Degree of analysis capacity • Formal versus informal information-exchange • Use of social media tools, short message services • Degree of cooperation with private services
'main barrier trust'	• Degree of mistrust in general • Degree of experience ('Chicken-egg dilemma') • degree of reluctance between law enforcement and intelligence services • lack of awareness due to information gap
'interoperability of used IT-systems'	• Interconnectivity of IT-systems used by Europol • Access to IT-systems with an added value • Degree of data collation • Links and connectivity between law enforcement and intelligence services
'effectiveness of an integrated information management system'	• Degree to identify potential terrorists • Degree to identify persons involved in terrorism-related activities • Degree to identify rapidly trends, immediate and long-term threats

8.2 Interview Guide

1. Does your management articulate the need for information exchange with the member states as an important issue that should be expanded?
2. Do you think that the systems you use are appropriate for the exchange of data (at Europol and within the EU)?
3. Concerning the increased data collection, do you think that Europol is prepared to manage the analysis of masses of data?
4. To accelerate an ongoing investigation, do you use formal or informal communication channels?
5. What will change with the new regulation for Europol, enter into force as from 1st May 2017?
6. Police officers use increasingly messenger services for exchange. What is your opinion concerning obstacles and advantages? Would you recommend such apps special tailored for police?
7. What about the use of social media analysis tools?

8. Which data systems do you mainly use in your daily work?
9. How do you assess the interconnectivity of IT-systems at Europol in general?
10. Do you have access to the main IT-systems according to your opinion?
11. How do you assess the current data collation? Recommendations for improvement?
12. What about the connections to intelligence services? To what extent are they implemented and with which tools?

13. Do you think that 'trust' is an important precondition for information exchange? Or vice versa do you think that 'mistrust' can be linked to an information gap?
14. What is according to your opinion the reason for the lack of cooperation between law enforcement and intelligence services?
15. Is there according to your opinion a relation between 'experience' and 'trust'?

16. What preconditions needs to be fulfilled to have an effective 'integrated information management system?
17. Is the current used information system within the EU able to identify short and long term threats?

18. Do you think that the current used information system is sufficient to detect potential terrorist or criminals?
19. How do you appraise the declarations by the EU to force the implementation of an integrated information management system?

8.3 List of conducted Expert Interviews in Chronological Order

-----The transcripts of the interviews have been deleted to guarantee the anonymity of the interview partners-----