Following illicit finance across distance and difference

The coordination and practices of financial intelligence units

Lagerwaard, P.

Publication date
2023

Document Version
Final published version

FOLLOWING ILLICIT FINANCE ACROSS DISTANCE AND DIFFERENCE

The Coordination and Practices of Financial Intelligence Units

PIETER LAGERWAARD

FOLLOWING ILLICIT FINANCE ACROSS DISTANCE AND DIFFERENCE

The Coordination and Practices of Financial Intelligence Units

Pieter Lagerwaard

ISBN 978-94-6473-055-5
Cover Guus Lagerwaard
Layout Ilse Modder; www.ilsemodder.nl
Printed by Proefschriften.nl

Following Illicit Finance across Distance and Difference

The Coordination and Practices of Financial Intelligence Units

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
prof. dr. ir. P.P.C.C. Verbeek
ten overstaan van een door het College voor Promoties ingestelde commissie,
in het openbaar te verdedigen in de Aula der Universiteit
op vrijdag 31 maart 2023, te 14.00 uur

door Pieter Lagerwaard
geboren te Amsterdam

Promotiecommissie

Promotor:	prof. dr. M. de Goede	Universiteit van Amsterdam
Copromotor:	dr. R. Bellanova	Universiteit van Amsterdam and Vrije Universiteit Brussel
Overige leden:	prof. dr. A. Leander	Geneva Graduate Insitute
	dr. A. Amicelle	Sciences Po Bordeaux
	prof. dr. D.K. Mügge	Universiteit van Amsterdam
	dr. B. Bodó	Universiteit van Amsterdam
	prof. dr. S. Milan	Universiteit van Amsterdam
	dr. M. Hoijtink	Vrije Universiteit Amsterdam

Faculteit der Maatschappij- en Gedragswetenschappen

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (research project 'FOLLOW: Following the Money from Transaction to Trial', Grant No. ERC-2015-CoG 682317).

“God is in the details, and so is everything else—including the Devil”
- Latour, 2007, p. 137

Table of Contents

Previous Publications

This dissertation includes the following publications:

Chapter 3 – Lagerwaard, P. (2022). Financiële surveillance en de rol van de Financial Intelligence Unit (FIU) in Nederland. *Beleid en Maatschappij*, (49)2, 128-153. It has been translated from Dutch to English by Liz van Gerrevink-Genee.

Chapter 3 – Lagerwaard, P. (2023). Financial Surveillance and the Role of the Financial Intelligence Unit (FIU) in the Netherlands. *Journal of Money Laundering Control*, (26)7, 63-84.

Chapter 4 – Lagerwaard, P. (2020). Flattening the International: Producing Financial Intelligence Through a Platform. *Critical Studies on Security*, 8(2), 160–174.

This dissertation includes the following draft articles:

Chapter 5 – Lagerwaard, P. (Resubmitted). Circulating Knowledge Through Disparate Practices: Insights from the Global Pursuit of Terrorist Financing by Financial Intelligence Units. *Science as Culture*.

Chapter 6 – Lagerwaard, P. & De Goede, M. (Forthcoming). In Trust we Share: The Politics of Financial Intelligence Sharing. *Economy and Society*.

Abbreviations and Acronyms

AFM	Dutch Authority for the Financial Markets
AIVD	Netherlands General Intelligence and Security Service
AML	Anti-Money Laundering
AMLD	Anti-Money Laundering Directive
ANT	Actor-Network Theory
CTF	Counter Terrorist Financing
DNB	Dutch Central Bank
ECOFEL	Egmont Centre of FIU Excellence and Leadership
EFIPPP	Europol Financial Intelligence Public-Private Partnership
ERC	European Research Council
ESW	Egmont Secure Web
EU	European Union
FATF	Financial Action Task Force
FEC	Financial Expertise Centre
FIOD	Fiscal Information and Investigation Service
FIU	Financial Intelligence Unit
GDPR	General Data Protection Regulation
HOFIU	Head of FIU
IMF	International Monetary Fund
IR	International Relations
IS	Islamic State
ISCW	Social Affairs and Employment Inspectorate
MIVD	Military Intelligence and Security Service
NCTV	National Coordinator for Security and Counterterrorism
NTFIU	National Terrorist Financial Investigation Unit
PNR	Passenger Name Records
PPP	Public-Private Partnership
RIEC	Regional Information and Expertise Centre
SAR	Suspicious Activity Report
SCTF	Serious Crime Taskforce
STS	Science and Technology Studies
SWIFT	Society for Worldwide Interbank Financial Telecommunication
UN	United Nations
WB	World Bank
WODC	Research and Documentation Centre of the Dutch Ministry of Security and Justice
Wwft	Anti-Money Laundering and Anti-Terrorist Financing Act (Netherlands)

Figures, Tables, and Boxes

Figures

Tables

Boxes

1|

Introduction

1.1 Introduction

In July 2022, representatives of hundreds of Financial Intelligence Units from around the globe gathered in Riga at a conference with the intriguing name "Worlds Apart".[1] Financial Intelligence Units – often abbreviated simply as FIUs – are relatively new national government organizations that monitor financial transactions in order to combat security threats, such as money laundering and terrorism financing. The conference name "Worlds Apart" is telling, because FIUs are indeed diverse organizations that operate in varied and unique political, cultural, and economic environments. Moreover, they operate in different legal jurisdictions, each with its own regulations concerning issues such as privacy, data handling, and human rights. That FIUs are 'worlds apart', is therefore no understatement: despite their similar objectives – combatting crime by analyzing financial transactions – they operate in different worlds that do not always easily align.

And yet, to obtain access to information on transnational money flows and follow illicit finance around the globe, FIUs are bound to join forces, coordinate their operations, and exchange their expertise and financial intelligence. Because financial transactions flow irrespective of national borders, FIUs rely on timely information from counterparts. At present, 166 FIUs from different continents share financial intelligence via a joint international organization called the Egmont Group of FIUs. Through the

1 The "Worlds Apart" conference was part of the annual plenary of the Egmont Group of FIUs. See https://egmontgroup.org/news/news-release-financial-intelligence-unit-of-latvia-hosts-worlds-apart-during-28th-egmont-group-plenary/, consulted August 2, 2022.

Egmont Group, FIUs coordinate their operations and commit to fostering "the widest possible co-operation and exchange of information with other Egmont Group FIUs on the basis of reciprocity or mutual agreement" (Egmont Group, 2013, p. 8). In addition, FIUs exchange intelligence bilaterally and within regional partnerships. In the European Union (EU), for instance, FIUs share case expertise and financial intelligence through the FIU.net, a decentralized computer network hosted by Europol.

Given that FIUs are relatively new organizations, little is known about their operations, either within their national jurisdictions or in their collective pursuit of illicit finance via regional and global exchanges of financial intelligence. This dissertation examines how this collective of diverse security organizations overcomes geographical distance and works across operational barriers to share financial intelligence. Existing research draws attention to the broader 'chain of security' of which FIUs are part (De Goede, 2018), the challenges inherent in the international devices and networks that FIUs rely on (Amicelle & Chaudieu, 2018), and the unstable legal foundations of FIU intelligence exchange (Mouzakiti, 2020). Yet, the daily practices by which FIUs operate within their own national security chain, share their financial intelligence with foreign counterparts, and engage in transnational operations remain obscure. In this dissertation I zoom in on the *practice* of financial intelligence sharing – the daily operations of FIUs and experiences of practitioners therein, including the challenges, dilemmas, negotiations, conflicts, and political stakes. I am interested in how FIUs manage to share financial intelligence, despite the different environments in which they are embedded. I am interested in how different ways of practicing financial intelligence connect and assemble transnationally, to eventually generate intelligence that security actors can mobilize in criminal investigations. In sum, this research examines how the 'worlds apart' meet in practice and how FIUs work across these different worlds. The main research question is: *How do FIUs coordinate their operations transnationally and exchange financial intelligence across geographical distance and organizational difference?*

The use of financial transaction information in criminal investigations is a relatively new phenomenon. Indeed, it was inconceivable decades ago when payment infrastructures and spending behavior were primarily cash based and therefore left little if any digital trace. At present, commercial actors, such as banks and money transmitters, have amassed large digital databases of financial transactions.[2] Pursuant to national and international anti-money-laundering and counterterrorist financing legislation,[3] these

2 See for a complete list of reporting entities in the Netherlands, https://www.fiu-nederland.nl/en/to-report/do-i-have-a-duty-to-report; https://www.fiu-nederland.nl/nl/melden/ben-ik-meldplichtig, consulted January 5, 2022.

3 The Financial Action Task Force (FATF) formulates international recommendations, also called 'standards'. These are often implemented through regional regulatory frameworks, such as the Anti-Money Laundering Directive of the EU, which is at the time of this writing in its 6th version (AMLD 6). This directive, in turn, is translated into national legislation, such as the Wwft in the Netherlands (the law to prevent money laundering and terrorism financing).

actors have been made responsible for monitoring their databases and reporting unusual transactions to the FIU. This has rendered banks as security actors, Bosma (2022, p. 16) argues, that are held accountable for combatting threats such as terrorist financing. As De Goede (2017a, p. 21) observes, banks increasingly operate "in the frontline" of security operations such as countering terrorist financing. In the Netherlands alone, banks employed, at the time of this writing, an estimated 12,000 employees tasked to conduct client research, monitor transactions, and send information about unusual transactions to the FIU. This number is equivalent to about one in five bank employees (Kamphuis, 2021).

Whereas the academic literature has focused on the new security roles of private companies (Abrahamsen & Leander, 2016; Cutler et al., 1999; Helgesson & Mörth, 2019; Leander, 2013, Williams, 2010), far less is known about how *public* actors, such as FIUs, mobilize commercial, private financial data (with notable exceptions, e.g., Amicelle, 2017; Amicelle & Chaudieu, 2018; Mouzakiti, 2020). This is remarkable because FIUs play a pivotal role in between private and public security actors. Functioning as a buffer, the FIU is the only governmental organization that receives suspicious transaction information from commercial reporting entities. As such, FIUs are an essential part of what De Goede (2018) calls the 'chain of security', whereby transaction information travels and is translated from commercial actors, such as banks, to the FIU, and then possibly on to the police, to eventually in some cases be used as evidence in a court of law (see, e.g., Anwar, 2020). However, knowledge of how FIUs operate in this chain of security is, to date, scarce. Little is known, for instance, about "how FIUs handle, share, and analyse unusual transaction reports" (De Goede 2018, p. 35).

It is important to study the national and transnational operations of FIUs, because financial intelligence reveals private and often sensitive information about individuals and companies. The reports that FIUs receive from private actors concern not only transactions, but also addresses, telephone numbers, bank accounts and personal details, such as names, birthdates, driving license information, and other types of information from both open and closed sources. As Ferrari notes:

> Triangulated with other personal data points, [financial transactions] allow to infer information about individuals' activities, purchases and geographical movements, from which, in turn, sexual orientation, health status, religious and political beliefs and cultural preferences can be derived (Ferrari, 2020, p. 522).

Yet, FIUs receive this transaction information from reporting entities without clients' knowledge, and can share the information both nationally and internationally, similarly without informing the – not officially charged – 'suspicious subject'. Financial intelligence gathering therefore impacts the privacy of everyone with a bank account.

Without notification, citizens can come under scrutiny, and their personal (financial) data may be stored in databases and shared with organizations around the globe.

This dissertation focuses on the practices of FIUs, the daily operations and experiences of practitioners and their challenges, dilemmas and stakes. However, this produced an analytical and methodological challenge: how does one study transnational processes in daily practice, when actors are scattered around the globe? What practices are worth considering, when 166 FIUs engage in countless interactions, both bilateral and multilateral? The question of how to study transnational and global processes in daily practice has received considerable attention within a diversity of disciplines, such as science and technology studies (STS) (Bowker & Star, 2000; Latour, 2007; Law, 1986, 2002), international relations (IR) (Barry, 2013; Bueger & Gadinger, 2014; Leander, 2021; Salter, 2015), and what can be roughly defined as the anthropology of globalization (Appadurai, 1996; Tsing, 2005). Speaking to these literatures, the conceptual approach of this dissertation contributes to the study of large-scale transnational or global processes in practice, by making three analytical moves. First, the research moves from studying cooperation to studying *coordination*, in order to account for the coexistence of different realities of financial intelligence, how these entangle, and how they are continuously reordered and reassembled across geographies. Second, it places particular emphasis on the *materiality* of transnational processes, including the role of non-human actors such as software programs, meeting rooms, and numbering practices. Third, it proposes to study *vantage points*.

The empirical chapters, four in total, use different vantage points; that is, each adopts a different advantageous point, providing a view on practices whereby transnational processes are coordinated, political negotiations take place and power relations are reconfigured. Taken together, the various vantage points – explained further below – have enabled me to conduct qualitative research of transnational, global processes. The vantage points were selected through iterative fieldwork, including 29 interviews with 37 practitioners; participant observation at conferences, workshops, and seminars; and document analyses encompassing meeting minutes, annual reports, legal regulations, and policy reports, amongst others.

After an elaboration of the methodology in Chapter 2, these vantage points are presented in chapters 3 through 7. Chapter 3 adopts as a vantage point *FIU-the Netherlands* in order to understand how the financial intelligence that FIUs exchange is produced in practice, via FIUs' three core tasks: collecting, analyzing, and disseminating intelligence. Chapter 4 adopts as its vantage point the EU Commission Expert Group the *EU FIUs Platform*, to discern how dispersed FIUs produce and navigate common understandings of data sharing. Chapter 5 adopts the *numbering practices* of FIUs as its vantage point, to reveal how these provide FIUs a depoliticized, technocratic vocabulary through which cross-border operations can be coordinated. Chapter 6 adopts as its vantage point *circuits of trust*, to understand how informal relations and

complex political negotiations between FIU practitioners contribute to make financial intelligence shareable. Chapter 7, in conclusion, argues that it is the informal nature of international agreements in combination with the operational autonomy of FIUs, that makes it possible for FIUs to coordinate their operations and transfer privacy-sensitive financial intelligence across distance and difference. This chapter raises crucial questions of institutional oversight, accountability, and proportionality of FIU operations, that will be of interest to politicians, policymakers, and practitioners (see Table 7.1).

This introduction chapter continues as follows. First, it elaborates on the operations of FIUs, describing their core operations and the building blocks of the international context in which they operate. It then discusses existing literatures dealing with the use of financial transaction information for security purposes, including the literatures from critical security studies, surveillance studies, and international relations. Building on these literatures, the chapter presents the conceptual approach of this research and its three analytical moves. Finally, an outline of the remainder of this dissertation is presented, including the sub-questions that each of the empirical chapters raises and seeks to answer.

1.2 The FIU as novel security actor

> Countries should establish a FIU that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and financing of terrorism, and for the dissemination of the results of that analysis (FATF, 2022, p. 24).

Since the 1990s, countries around the globe have established Financial Intelligence Units (Amicelle, 2020). As one of my interviewees stated, the FIU is a novel security actor because it is "a new kid in town, with a new topic" (Former head of FIU, September 6, 2018). The FIU plays a pivotal and indispensable role in the surveillance of payment systems and spending behavior, because it operates at various intersections. It operates not only at the intersection of *finance* and *security*, but also at the intersection of the *private* and *public* spheres, working closely with commercial financial institutions that send it transaction information, as well as with the public actors that use the intelligence it produces. Furthermore, it operates at the intersection of *information* and *intelligence*, by collecting and connecting different types of data – not only financial – and transforming these through analyses into intelligence that is suitable for dissemination to security actors further down the chain. Finally, it operates at the intersection of the *national* context, in which each individual FIU collects, analyzes, and disseminates intelligence within its own particular jurisdiction, and the *international* security context, in which

FIUs have autonomy to independently share financial intelligence with 166 counterparts across continents via the Egmont Group. This section first discusses the role of the FIU in the national chain of security actors, after which it sketches the broader transnational context of which FIUs are part.

Core operations of an FIU

Nationally, an FIU is the chief organization that *collects, analyzes,* and *disseminates* financial intelligence. Commercial reporting entities, such as banks, are indispensable for *collecting* financial information; they provide the financial information that the 'chain of security' relies on (De Goede, 2018). Not only do banks and money transmitters (have to) report unusual financial transactions, but a plethora of other commercial private actors are obligated to report as well, including accountants, lawyers, real estate agents, juridical service providers, investment companies, cryptocurrency traders, casinos, and sellers of many types of luxury goods, such as gold, diamonds, cars, boats, and art. Figure 1.1 presents an example of the type of information that reporting entities are required to send to the FIU, in this case via the software GoAML, which is the software recommended by the United Nations for FIUs. It shows that the information commercial actors send is not only financial but includes many other details, often being supplemented by research based on both open and closed sources (FIU-Nederland, n.d.). The exact structure and content of the reports differ per country, yet all reports include a wealth of information beyond only financial data or clearly related to the financial transaction itself.

The *analysis* of these reports differs per FIU. Some FIUs analyze their data using highly advanced software, while others conduct primarily manual investigations (see, e.g., EU FIUs Platform, 2016). Some FIUs automatically disseminate reports to partners further down the security chain, while others investigate reports themselves first and filter through only those they consider relevant for particular security partners. Moreover, such analyses are not necessarily linear but may be *source-based*, meaning that the collected reports are gathered in a database and stored there for a number of years, resembling a 'pond' of data accessible primarily to the FIU to fish in. In such source-based analyses, each report is not analyzed separately when it enters the FIU. Rather, the entire database is periodically and systematically searched on the basis of new queries. This analysis approach may differ per FIU, entailing more or less automatic, semiautomatic, and manual methods of searching the database. Yet, despite their different approaches, all FIUs actively mediate the financial information they receive, translating it into intelligence that is (made) suitable for the FIU's partners further down the security chain.

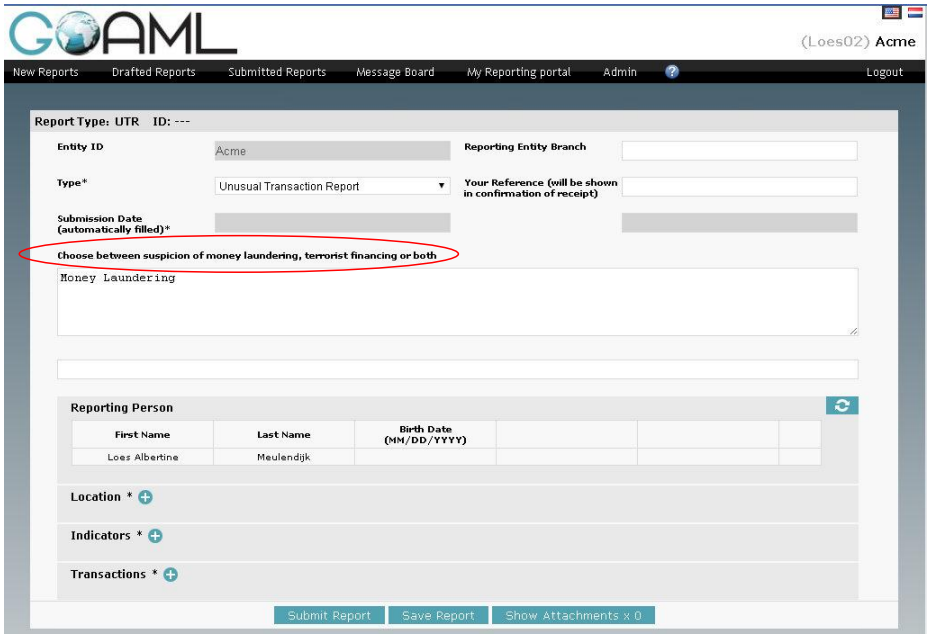


FIGURE 1.1 : First page of an STR report via GoAML in the Netherlands. This is a fictional example from a document from FIU-the Netherlands (n.d., p. 5).

The *dissemination* of intelligence, again, varies per FIU, but all FIUs share their intelligence with a range of domestic public actors in law enforcement, secret services, and occasionally, tax agencies or public prosecutors. Some FIUs' primary task is to smoothly relegate the intelligence to the right public partners, while others have active roles in the criminal investigations themselves, taking for instance part in public-private partnerships in which they cooperate with private actors and public security organizations on specific security threats, such as terrorist financing (Bosma, 2022). However, in general, FIUs do not have executive authority and are not allotted powers to search premises, make arrests or detain suspects. Their primary task is to generate intelligence that can feed into other investigations – a task that can be performed mostly from in front of a computer screen. Amicelle (2020) argues that because FIUs are new security actors with a new type of intelligence, their financial intelligence initially did not fit the operations of traditional security actors, such as secret services and policing institutions. Over time, FIUs have sought to stimulate demand for their financial intelligence, by spreading the word that they have novel intelligence to offer to security agencies.[4]

Despite their different ways of collecting, analyzing, and disseminating

4 See, e.g., this promotional video from FIU-the Netherlands: https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/afbeeldingen/32964_fiu_uk_v4.mp4.mp4, consulted July 29, 2022.

intelligence, all countries have a similarly structured system of financial intelligence in place, with an FIU in between private and public actors. However, the FIUs' interpretation and implementation of their task, in terms of who should report, what should be reported, how reports should be dealt with, and what security actors should eventually receive intelligence, vary considerably from country to country. These organizational and institutional differences are observed in the number of reports that FIUs handle. For instance, between 2006 and 2015, Germany's FIU received 117,217 reports, while that of France received 188,570 reports, and that of Spain received 28,046 reports (Europol, 2017). These numbers are considerably lower than, for instance, the UK, where the FIU received 2,329,609 reports (ibid.). The FIU of the Netherlands is a particularly striking example. Between 2006 and 2015, it received 2,026,299 reports, which is 17 times more than its (economically larger) neighbor Germany – and even far more than Germany, France, Spain, and Italy combined (ibid.). The Netherlands and UK accounted for 67% of all reports in the EU member states between 2006 and 2015 (Europol, 2017, p. 10). These differences are not indicative of more financial crime in the UK and the Netherlands, or of the two countries having necessarily better systems in place to detect financial crime. Instead, these diverging numbers reflect the different organizational structures and institutional environments in which the FIUs are embedded: the unique economic, political, cultural, and legal contexts of the national jurisdictions in which they operate.

Sharing financial intelligence

The FIU plays a pivotal role in the chain of security, because it has the authority to share its intelligence with other FIUs internationally. As mentioned, FIUs join forces via their international platform, the Egmont Group, which has grown substantially, from 13 members in 1995 to 166 members in 2022 (Egmont Group, 2015, 2022b).[5] A member can share domestic information with counterparts, but in return it can request and receive financial intelligence from foreign FIUs. Intelligence from abroad can then be combined with or added to its own national database and disseminated further down the national chain of security. Because FIUs are very different organizations, operating in diverse and unique legal and political environments, this exchange of intelligence poses significant challenges. According to Amicelle and Chaudieu (2018, p. 666), the different devices and channels that FIUs use to communicate and share financial intelligence, give rise to tensions, associated with "a lack of capacity to respond to a request,… the low level of spontaneous dissemination, or to 'abusive' restrictions on the use of information". Furthermore, Mouzakita (2020, p. 3) points out challenges regarding data protection, showing how as a result of the different legal frameworks in which FIUs operate, their financial intelligence may be subject to conflicting regulations when it

5 For current membership numbers, see https://egmontgroup.org/about/, consulted August 3, 2022.

travels from one FIU to another.

The main legal basis for FIU operations is formed by the recommendations of the intergovernmental Financial Action Task Force (FATF) and the regulatory documents of the Egmont Group. The FATF has developed 40 recommendations for implementing financial intelligence, which are often also referred to as 'standards' (FATF, 2022). It has also developed nine recommendations dealing specifically with terrorist financing (FATF, 2001). Initially, the FATF was founded and governed by a small group of 'Great Powers', mainly the US and its allies (De Oliveira, 2018; Jakobi, 2018). Yet nowadays, large non-Western economies, such as China, Russia, Turkey, India and Brazil, are all part of its main governing body. With the exception of Iran and North Korea, all countries in the world recognize and implement the FATF recommendations. The FATF does not have the power to enforce standards, and it is often portrayed as an apolitical organization that operates on the basis of experimentalist governance (Nance, 2018). Yet in practice, the organization applies "invasive" mutual evaluations (Nance 2018, p. 118), by which on a rotating basis countries evaluate on another's implementation of the FATF standards. The FATF can exercise substantial influence by placing certain jurisdictions under increased monitoring. In 2021, Syria, Pakistan, Botswana, Cambodia, Morocco, and Zimbabwe – among others – were placed on what is often called the 'grey list' and subjected to additional monitoring. Iran and North Korea were on the blacklist. The power of the FATF derives primarily from the fact that these listings have substantial effect on a country's financial credibility and, hence, access to foreign capital on the international financial markets (see, e.g., Sharman, 2008, 2009).

The Egmont Group of FIUs builds on the FATF recommendations. It supplements these with additional regulatory documents, particularly its charter, guidance, and principles documents. When joining the Egmont Group, an FIU must indicate consent to abide by these regulatory documents, which underwrite several FATF recommendations. The most important of these is the 29th recommendation – the opening quote of this section – and the 40th recommendation (Egmont Group, 2017, p. 3). The latter states:

> Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing cooperation (FATF, 2022, p. 29).

The Egmont Group supplements these FATF recommendations with its own documents. The Egmont Group charter sets out the general definitions, purpose, and organization of the collective (Egmont Group, 2019); its principles document deals primarily with international exchanges of information between FIUs (Egmont Group, 2013); and its

guidance document delineates a general framework for FIU operations at both the national and international levels (Egmont Group, 2017).

To share financial intelligence transnationally, FIUs use either a software system that is made available by the Egmont Group, or through regional means of exchange. The Egmont software system is called the Egmont Secure Web (ESW). The Egmont charter describes this as "an electronic communication system that allows encrypted sharing among members of emails and financial intelligence, as well as other information of interest to members and to the functioning of the Egmont Group" (Egmont Group, 2019, p. 8). The ESW is hosted by the Financial Crimes Enforcement Network (FINCEN), which is the US FIU. Through the ESW, FIUs can communicate and share financial intelligence in a protected environment (see also Amicelle & Chaudieu, 2018). In addition, FIUs may share data and intelligence bilaterally and via regional cooperation hubs, such as the European FIU.net, which is hosted by Europol and connected to the servers of EU FIUs. The features of FIU.net are similar to those of the ESW, but the former offers more 'high-tech' features, such as an automatic monitoring system which connects and searches associated FIU databases based on filters (Kroon, 2013; Mouzakiti, 2020, pp. 10–13). Using one system does not exclude use of the other. FIUs can use both systems simultaneously, depending on which FIU they are exchanging intelligence with.

However, the practice of sharing intelligence transnationally does not rely only on the software systems in use or the recommendations of the FATF and regulatory documents of the Egmont Group. The recommendations and regulatory documents are not legally binding, nor are they enforced by any central authority with license to dictate rules and impose these on individual FIUs. Because the members of the FATF and Egmont Group have different interests and politics, which might not easily align, no official internationally binding legal treaties have been drafted regarding their activities, let alone signed. Therefore, the regulatory and legal foundations of transnational financial intelligence and the operations of FIUs are often formulated in imprecise and ambiguous terminologies, such as 'recommendations', 'principles' and 'guidelines', instead of, for instance, as international rules, laws, and treaties.

1.3 Existing research

This section discusses the existing research on which this research draws and to which it aims to contribute. In this regard, three academic conversations are key. Each is discussed separately below, despite the fact that they, to some extent, overlap. The first is the conversation on the relation between finance and security, found particularly in critical security studies and drawing attention to the 'securitization' of finance and the finance-security nexus (Boy et al., 2017). Second is the conversation about the extent to which the use of financial transactions for security purposes can be considered a

surveillance practice from the surveillance literature. The third conversation, from IR and cognate disciplines, such as international political economy, regards the political, geopolitical, and economic contexts of financial intelligence. After discussing these three scholarly conversations, this chapter will turn to the conceptual approach of this dissertation, its analytical moves, and how it aims to contribute to existing scholarship. In particular, by drawing from literatures at the intersection of STS and IR, it develops the notion of 'vantage points' to study the daily practices of transnational processes. The final section of this chapter provides an outline of the dissertation and discusses each of the vantage points and sub-questions in turn.

Critical security studies

The emergence of financial intelligence and its rapid spread around the globe follows a broader trend of the expansion of security logics to domains that were previously not considered security fields. Security, as a study area, used to belong primarily to disciplines such as IR, political science, and military studies. In contrast, the field of finance used to be considered primarily in relation to economics or politics, rather than as part of (national) security. The notion of security has thus 'widened' (Buzan & Hansen, 2010) and shifted to what is broadly known as 'human security' (Floyd, 2007), including security problems such as food security and health security. In the field of critical security studies, authors have taken stock of security in a diversity of contexts, such as the Anthropocene (Rothe, 2020), airports (Hoijtink, 2007; Salter, 2008), public controversies (Monsees, 2020), and migration control (İşleyen, 2018). This dissertation is interested in the nexus between *finance* and *security*, whereby financial transactions are seen both as a security problem and as a source of intelligence that can reveal unlawful activities and be used as a tool to preemptively counter these.[6]

The intersection between finance and security has received notable consideration from critical security studies scholars, who view the financial domain as another field that is, or has been, 'securitized' (Biersteker & Eckert, 2008; Boy, 2017; De Goede, 2012; Wesseling, 2013).[7] The concept of securitization is helpful here to understand how domains such as finance become perceived security threats. Building on securitization theory (Buzan et al., 1998), Floyd (2007, p. 42) observes three steps: the "(1) identification of existential threats (also known as securitizing moves), (2) emergency action, and (3) effects on inter-unit relations by breaking free of rules". Issues such as finance that were not formerly related to security are framed as security problems, thus making exceptional policy formulations possible. A growing body of literature focuses on the finance-security nexus (Boy et al.,

6 According to Amoore and De Goede (2008b, p. 174), the financial transaction "has become a specific preemptive means of securing in the face of an uncertain future". Situated against the War on Terror, these authors argue that the transaction is increasingly the basis on which security decisions are made (on preemption, see also Boy et al., 2011).

7 Amicelle (2017b, p. 222) rightfully argues that financial intelligence not only entails the securitization of finance, but also fosters the financialization of security.

2017) and inquires into the relation between security and debt (Langenohl, 2017a; also 2021), the concept of 'dirty money' (Amicelle, 2017b), and the relation between finance, security, and social welfare and wellbeing (Langley, 2007; also 2014). However, the nexus between finance and security also has historical roots. For example, De Goede (2010, p. 107) draws "attention to the joint histories, philosophies and technologies of governing through uncertain futures in what are often thought to be the separate domains of finance and security" (see also De Goede, 2017). Gilbert (2015, p. 203; see also 2017), furthermore, demonstrates that war and money co-constitute and operate as a "weapons system", whereby "militaries have always been deeply enmeshed in markets and economies, both domestically and in conflict scenarios".

Some critical security studies scholars have refined securitization theory by arguing that not only discourse and speech produce security problems, but that security and securitization are empirically produced by individuals through daily practices (Collective, 2006; Mutlu & Salter, 2014). Referring to the work of Booth (2007), Buzan and Hansen (2010, p. 9) write that critical security studies emphasize "an intersubjective definition insofar as individuals' own definitions of security problems should be taken into account". De Goede (2018, p. 32) follows a single transaction through the chain of security, demonstrating that the daily routinized practices of practitioners may consist of "countless small judgements". This exercise serves to illustrate that "financial transactions need to be inscribed in dossiers, analyzed, debated and modelled, in order to be rendered intelligible and valid as security facts" (ibid.). Furthermore, Amicelle (2017a, p. 1) questions the "everyday policing practices emanating from the configuration of social actors from finance-oriented institutions and security-oriented institutions". This author's (ibid., p. 2) study of the everyday practices of professionals demonstrates that practitioners engage in "productive misunderstandings" whereby actors "act as if they believe to agree on a common practice… although they do not meet and interact on the same ground of meaning".

Similarly, this dissertation examines daily practices of financial intelligence exchange and its transnational coordination. Studying practice has become an increasingly important approach in IR and critical security studies (Adler & Pouliot, 2011; Balzacq et al., 2010; Bueger & Gadinger, 2014). Bueger and Gadinger (2014, p. 3; also 2015) write that "a broad movement of scholars across the social sciences has started to think about practice and how the investigation of doing and sayings can provide us with a better understanding of the world". These authors speak of a 'practice theory', with which to bridge the divide between practice – "what 'normal' people are doing" – and abstract theory, arguing that "practice and theory are intrinsically linked: without practice, no theory, and vice versa" (ibid., p. 4). In other words, studying practice can provide rich empirical detail that enables the researcher to generate theory that is empirically substantiated and sound, and which might provide novel insights about broader issues and processes. As Adler and Pouliot (2011, p. 1) write, "by focusing

on what practitioners do, we zoom in on the quotidian unfolding of international life and analyze the ongoing accomplishments that, put together, constitute the 'big picture' of world politics". Practice scholars have inquired into the routinization of practices (Bueger & Gadinger, 2014, p. 61), the "point of practice" where practitioners act upon the world (De Goede, 2018, p. 38), and the social and material nature of practices (Law, 2016). What most practice scholars share, in particular in critical security studies, is the use of qualitative, often ethnographic methodologies to study the practice of (transnational) practitioners (Leander, 2015a; Salter & Mutlu, 2013).

With respect to this research's interest in the daily dilemmas and challenges of financial intelligence practitioners, critical security studies, with its emphasis on practices, offers tools to understand and situate the production of finance as a security issue by emphasizing the often repetitive and mundane activities through which it is constructed. Bonelli and Ragazzi (2014) demonstrate, for example, the importance of including 'low-tech' security practices, such as files, notes, and memos. The practice of financial intelligence sharing is a combination of human considerations and expertise as well as bureaucratic activities, such as gathering reports in digital repositories and analyzing and disseminating digital or paper files. To understand transnational processes, such as financial intelligence, this research accepts it as vital to consider the seemingly small and often technocratic practices that form the basis of international financial intelligence sharing and geopolitical security operations.

Financial surveillance

In the field of critical security studies, questions are thus increasingly being raised concerning the securitization of finance (Boy et al., 2017; De Goede, 2010; Gilbert, 2017; Langley, 2017). Yet, the use of financial transaction data for security purposes can also be approached as a *surveillance* practice. According to Lyon (2007, p. 14), surveillance is "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction". Salter (2010, p. 187) argues that surveillance practices are part and parcel of security studies, observing that "surveillance is the organized observation of behavior with the intention of care or control of the observed, and forms an important object of study in new security studies". Already in the early 2010s, Amicelle (2011, p. 162) argued that we need a new "political anatomy" of financial surveillance, one that takes into consideration the multitude of heterogeneous actors and their different goals (see also Amicelle & Favarel-Garrigues, 2012). Amicelle (2011, p. 162) distinguishes between different "professional worlds" that converge in this anatomy: the financial professionals, such as financial institutions and ministries of finance, and the security professionals, such as police departments and intelligence services. In this anatomy and these professional worlds, the FIU has an important position, not only because it is prominently positioned in the middle of the chain of security (De Goede, 2018; also 2017b), but also because it operates at various

intersections, as discussed above. For this reason, the FIU is pivotal and indispensable in the surveillance of payment systems and spending behavior. It arguably constitutes the beating heart of the political anatomy of financial surveillance.

However, financial intelligence and security actors such as FIUs, have only marginally been considered from a surveillance angle. While the general study of surveillance "has mushroomed" and is still expanding (Lyon et al., 2012, p. 1), FIUs' relatively novel modus of financial surveillance has been considered primarily in the context of surveillance of Islamic organizations (Atia, 2007) and terrorist financing (Vlcek, 2007, 2009). This is surprising, because surveillance studies includes a diversity of topics not limited to classic subjects, such as cameras (Armstrong & Norris, 1999) and the surveillance state (Weller, 2012). Surveillance studies covers important conceptual themes, such as the role of technologies and data (Bellanova, 2017; Bellanova & Fuster, 2013; Kazansky, 2021; Van Dijck, 2014), that are helpful in the study of financial intelligence.

It is useful to approach financial intelligence and FIUs from a surveillance angle, because financial intelligence is not only a targeted practice – for example, targeted at criminal organizations and terrorist groups – but relies on systemic and mass collection of (financial) information from society at large, in order to detect illicit activities. For instance, the Netherlands' FIU stores unusual transaction information in a database for five years, without informing the customer or client that conducted the transaction (see Chapter 3). This database of unusual transactions includes some 1.2–1.4 million reports (Akse, 2019, pp. 5–8) and is systematically searched in reference to national and international lists and on the basis of requests from investigative services. Only when an unusual transaction is flagged as suspicious, is it transferred to another database, that of *suspicious* transactions, which is accessible to the broader spectrum of police and certain investigative services and a targeted investigation may ensue. As a metaphor, the FIU can be thought of as an hourglass. Information on unusual financial transactions flows like sand from many private entities to the FIU, the core of the hourglass. After analysis, it sends modified intelligence to a wide breadth of security actors. However, the FIU does not let all the 'sand' pass; rather, it monitors, selects, modifies and filters what goes through.

Approaching financial intelligence as a surveillance practice offers useful ways of conceptualizing FIUs. While FIUs are not Orwellian organizations in the conventional sense, because they rely on *commercial* information (Orwell, 1949), they do belong to the government and are embedded in either a ministry, the police organization, the judiciary, or a combination of these (IMF and WB, 2004). Like Facebook and Google, FIUs rely on commercial data; yet, as a public actor they do not use that data in pursuit of commercial interests – which Zuboff (2019) calls "surveillance capitalism". FIUs are interested in financial information for security purposes: to surveil payment systems and transaction behavior in order to detect and prevent illicit activities. FIUs could be

seen as a classic payment 'panopticon' in a Foucauldian (or Benthamian) understanding (Foucault, 1977). However, most of society – at present – is unaware that their spending behavior is so extensively monitored and, hence, unlikely to self-discipline. Therefore, FIUs can perhaps best be understood as a 'surveillant assemblage', whereby information on clients is abstracted and reassembled in what Haggerty and Ericson (2000, p. 613) call "data doubles" which – without clients' knowledge – find purpose in various places in the security domain.

The analogy of the surveillance data double is useful to understand FIUs as the beating heart in the "political anatomy" (Amicelle, 2011, p. 162). Following Haggerty and Ericson (2000, p. 613), "data doubles circulate in a host of different centres of calculation and serve as markers for access to resources, services and power in ways which are often unknown to its referent". Some FIUs annually collect and store tens of thousands of transaction reports, others hundreds of thousands, and some even millions of reports – such as the FIU of the Netherlands. These reports are shared domestically with a wide range of security actors without the knowledge of the referent – the client. In addition, they are shared internationally with members of the Egmont Group who commit to "rapidly, constructively and effectively provide the widest range of international cooperation" (FATF, 2012, p. 29; see Egmont Group, 2019, p. 8). The intelligence, in this sense, duplicates or 'doubles', as it does not *leave* the FIU, but only a copy of the intelligence travels, translates, and circulates to a host of different places. FIUs may share sensitive information with countries that have questionable reputations concerning issues such as privacy and human rights, such as Syria, Saudi Arabia, Venezuela, Egypt, Belarus, Cuba, and Bahrain, all of which are members of the Egmont Group. Because intelligence travels without the knowledge of the client, potentially anyone with a bank account might have personal data circulating and doubling, both domestically to a range of security actors, as well as around the globe "to a host of different centres" (Haggerty & Ericson, 2000, p. 613).

However, according to De Goede and Bellanova (2022, p. 106), it takes hard work to make these types of data transportable and to "generate seemingly smooth dataflows". Furthermore, Beraldo and Milan (2019, p. 2) point out the "contentious politics of data", by which they refer to a bottom-up process of contesting "existing power relations and narratives and/or… re-appropriating data practices and infrastructure for purposes distinct from the intended" (see also Milan, 2019). To be successful, (mass) surveillance relies on stable data architectures, or infrastructures, that make data – such as in this case, financial intelligence – mobile across jurisdictions (Bellanova & De Goede, 2022; Gillespie, 2014; Star & Ruhleder, 1996).

International relations

Security and surveillance studies, respectively, help to elucidate the role of FIUs in the nexus between finance and security (Boy et al., 2017) and as the heart of the "political

anatomy" of financial surveillance (Amicelle, 2011). IR and related disciplines, such as international political economy, in turn, shed light on the political, geopolitical, legal, and economic contexts in which FIUs exchange intelligence. Practitioners working in financial intelligence tend to view FIUs as peculiar organizations that seem to be more loyal to one another than to their respective countries and governments (Financial crime consultant, October 16, 2018). Following international standards and guidelines, FIUs are by institutional design, granted considerable autonomy to operate independently and decide with whom to share intelligence, both domestically and transnationally. In theory, this autonomy detaches the FIU from its national government, thereby providing a safeguard against governmental interference and possible misuse of financial intelligence. However, that same independence renders FIUs 'peculiar' organizations, precisely because they answer primarily to one another, relying heavily on each other's intelligence to trace transactions across borders. Via the Egmont Group, 166 autonomous yet mutually dependent FIUs cooperate and share their sensitive financial intelligence with little intragovernmental supervision or national oversight.

The IR and international political economy literatures have mapped the pre-existing geopolitical architecture into which financial intelligence, having appeared on the global stage only in the 1990s, emerged. As such, modern global banking systems and financial institutions gave rise to what Best (2003) calls a "new financial architecture". This architecture has forced countries to subject themselves to a neoliberal ideology, according to Best (ibid.), and stimulated what scholars refer to as the 'financialization' of economic accumulation (see, e.g., Blackburn, 2008; Krippner, 2005; Langley, 2007). This new financial architecture is important to consider in order to understand transnational financial intelligence, because some of its core institutions, such as the International Monetary Fund (IMF) and World Bank, are or have been actively shaping financial intelligence governance. Both the IMF and World Bank, for instance, have served as observer organizations in devising FATF recommendations (FATF, 2022, p. 8), and they have published influential reports such as on the organizational structures of FIUs (IMF and WB, 2004).

Furthermore, IR has used financial intelligence as an example to raise new questions about present-day global governance (Boy et al., 2011; De Oliveira, 2018; Hülsse & Kerwer, 2007; Mügge, 2014; Nance, 2018; Vlcek, 2012). For instance, Vlcek (2012) points to the importance of the FATF's role in global financial governance, demonstrating that in the Philippines the FATF evaluations have had severe impact on capital flows, particularly affecting migrants. Drawing on Sharman (2009), Vlcek (2012, p. 655) observes that "even states with little need for anti-money laundering legislation will enact such legislation because of the negative consequences for failing to demonstrate that international standards in this area have been met". De Oliveira (2018), furthermore, claims that global governance is influenced by the entanglement between public and private security actors, and that this has gradually undermined the

influence of states in transnational organizations such as the FATF. The governance of financial intelligence illustrates, according to De Oliveira (ibid.), that the shift from a 'rule-based' system to a 'risk-based' system has worked in favor of private sector enterprises, as power is now distributed among a variety of public and private national and transnational actors.

The FATF recommendations tend to travel via regional legislation into national legislation. For instance, in the EU, the Fifth Anti-Money Laundering Directive (5-AMLD) draws on the FATF recommendations and is, in turn, translated into national legislation, such as the Netherlands' Anti-Money Laundering and Anti-Terrorist Financing Act (known by the acronym *Wwft*, from the Dutch name).[8] As a result, transnational financial surveillance entails a patchwork of differently organized legal, operational, and regulatory jurisdictions that are embedded in unique political and institutional contexts. According to Nance (2018, p. 113), money laundering regulations pose a "fundamental challenge of global governance today…. Those seeking to regulate it… are bound by traditional conceptualizations of sovereignty and held back by the legal boundaries of their jurisdictions". It is in this complex and multifaceted context that FIUs need to coordinate their operations.

1.4 Conceptual approach

This research draws on literatures at the intersection of STS and IR to unpack the daily practices of transnational financial intelligence exchange. Whereas STS addresses the importance of science and technology, the mediating role of non-human actors, and the significance of materiality, IR has a rich history in the study of processes of broader international and global scope, with particular emphasis on governance, political stakes, and power relations. Increasingly, scholars are exploring this intersection by studying the international nature of objects (Salter, 2015, 2016), translations (Barry, 2013; Best & Walters, 2013; De Goede, 2018), technology (Hoijtink & Leese, 2019), infrastructures (Aradau, 2010; Bellanova & Glouftsios, 2022), and topics such as security (Bellanova et al., 2020; Walters, 2014) and migration (Dijstelbloem & Walters, 2021; Van der Kist et al., 2019). In this dissertation I seek to contribute to these literatures by addressing a core issue that arises at this intersection: How does one study processes of grand scale and scope, spanning the globe, such as the exchange of financial intelligence by FIUs, by turning to situated, arguably 'small' practices?

This issue has been addressed in STS, particularly, by actor-network theory scholars (Bowker & Star, 2000; Latour, 2007; Law, 1986, 2002), as well as in IR (Barry,

8 Wwft stands for Wet ter voorkoming van witwassen en financieren van terrorisme (the law to prevent money laundering and terrorism financing).

2013; Bueger & Gadinger, 2014; De Goede, in Salter et al. 2019, p. 31; Salter, 2015), and the domain that can be roughly termed the anthropology of globalization (Appadurai, 1996; Tsing, 2005). According to Latour (2007, p. 5), actor-network theory scholars should study how larger group formations come into being by tracing the *associations* between different actors – not only human actors but also non-human (material) actors. In IR, impressive studies have been conducted on large-scale formations by scholars tracing how material objects *circulate* (Salter, 2015, p. ix). This literature reveals objects such as tanks (Shapiro, 2015), but also mundane objects like garbage (Acuto, 2015), to be not passive elements but as shaping and mediating what we know as 'the international' (Salter, 2015, 2016). Somewhat in contrast, Appadurai (1996) proposes to engage in a "transnational anthropology" that does not focus on specific material objects but rather on certain "scapes", such as the ethnoscape, the mediascape, and the technoscape, which work all the way down to the level of the individual. According to Appadurai (ibid., p. 33), "the individual actor is the last locus of this perspectival set of landscapes, for these landscapes are eventually navigated by agents who both experience and constitute larger formations".

Speaking to these literatures, this dissertation makes three analytical moves to study transnational processes in practice.

From cooperation to coordination

First, this research shifts the analytical focus from cooperation between a limited number of actors to coordination between multiple actors. Drawing in particular on Mol (2010), I use the notion of coordination to understand how different realities of financial intelligence co-exist, including a multitude of actors that are entangled with one another and therefore in one way or another *have to relate* to each other, though this is not always achieved smoothly. As observed before, FIUs operate in unique environments that do not merely generate different interpretations of financial intelligence, but construct different socio-material realities of what financial intelligence and security threats are. Threats, such as terrorist financing, are *defined* differently, with FIUs labelling different regions or groups as suspected of terrorist activity (Schmid, 2004; Sorel, 2003). In addition, terrorist financing is *measured* and *categorized* differently, with some FIUs using stringent indicators while others rely on generic ones (Europol, 2017). Terrorist financing is *counted* differently, with some FIUs labeling each transaction separately, while others register bulks of transactions in files. Yet, in order to pursue illicit finance across borders, it is pertinent for FIUs to bridge these organizational differences in order to exchange financial intelligence.

It is in this context of 166 FIUs and a plethora of actors involved, that the concept of coordination offers an analytical advantage. Mol (2002, 2010), who spells the word using a hyphen (co-ordination) for an analytical reason, conducted research on the disease atherosclerosis in a Dutch hospital. Mol (ibid.) found that different 'versions'

or 'realities' of the disease relationally coexisted: the patient, surgeon, and pathologist enact the disease in different ways. From this angle, an object, such as a disease, is not being interpreted in different ways – akin to conventional interpretivism, which focuses on how the same object can give way to a plurality of interpretations (Geertz, 1973) – but it actually *exists* and is brought into being in multiple entangled ways. Because an object is decentered and assumed to exist in a variety of ways in different places, multiplying and scattering the production of reality, the political becomes a question of how these realities relate, tie together, and involve an "ontological politics" (Mol, 1999). Studying coordination is helpful to understand how these multiple realities connect and entangle:

> As soon as attention shifts to the co-existence of different realities (or logics, or modes of ordering) the question arises as to how these hang together. The term co-ordination is helpful here, since it does not evoke a single, overarching and coherent order in which everything fits just fine and friction-free like the bits and pieces of a mosaic or the components of a watch. Instead, the term co-ordination suggests continuing effort. Tensions live on and gaps must be bridged, hence the need for "co-ordination" (Mol, 2010, p. 264).

By insisting on the hyphen, co-ordination refers both to the practice of coordination between a multitude of elements, as well as to the relational dimension of this as a *co*-endeavor. Furthermore, the concept subtly refers to the notion of coordinates; that is, objects' geographic positionality in the world (and their relative distances).

Not only are FIUs organizationally diverse and their political and legal environments unalike, but the ways in which they actually generate financial intelligence and bring security threats such as terrorist financing and anti-money laundering into being, constitute different realities. FIUs use diverse definitions of security threats and apply different standardizations, procedures, and protocols. They also use different methods to quantify unusual or suspicious transactions. This results not in different interpretations of a singular static object, but in different versions of financial intelligence, different realities of what threats such as terrorism financing are, and how they can be combated. In a similar manner as Mol's study of how different versions of atherosclerosis entwined in the Dutch hospital, this dissertation seeks to unpack how multiple realties of financial intelligence are constructed and co-ordinated in the transnational practice of exchanging intelligence. It investigates how FIUs co-ordinate these realities and manage to work across them in daily practice. I do not assert that this co-ordination runs smoothly or as planned. In fact, struggles, conflicts, and misalignments may mean that hard work is required for intelligence to travel from one jurisdiction to another (see, e.g., Bellanova & De Goede, 2022; Pelizza, 2016).

As Mol (2010, p. 264) points out, a challenge inherent in the concept of co-ordination is that "it may seem to suggest that someone somewhere is deliberately and mindfully engaged in co-ordination work". As scholars in actor-network theory have shown (Aradau, 2010; Barry, 2013; Callon, 1984; Harman, 2009; Latour, 2007), there is seldom one core actor that mobilizes the rest – or, put differently, one thing or person that *does* the co-ordination. Rather, as Latour (2007) suggests, it is possible to trace *associations* between different actors, both human and non-human:

> For ANT [actor-network theory], as we now understand, the definition of the term [social] is different: it doesn't designate a domain of reality or some particular item, but rather is the name of a movement, a displacement, a transformation, a translation, enrollment. It is an association between entities which are in no way recognizable as being social in the ordinary manner, except during the brief moment when they are reshuffled together (Latour, 2007, pp. 64–65).

Actor-network theory is not so much about the network or the actor, but following Latour (2007), about the associations between the actors that make up a network. Studying associations is key regarding co-ordination, I assert, because actors do or are made to do things *in relation to* one another. In this sense co-ordination is not a centrally orchestrated affair, in which one key thing or person has the power to pull all the strings. Rather, it is a connected network of actors which influence one another. The term 'associations' is not rigid or static here, or the only one possible. Mol (2010, p. 259) suggests that we could think of other terms to denote how actors stand in relation to one another, such as "collaboration, clash, addition, tension, exclusion, inclusion, and so on". The crux is that, in any given affair, a plethora of actors *relate* to each other and are a part of and influence – to a greater or lesser extent – the networked co-ordination.

In contrast to cooperation, which seemingly takes place in a relational vacuum between two or three entities, the term of co-ordination is particularly valuable to understand transnational processes, I argue, because it enables the researcher to include the many actors and associations involved across a potentially grand geographical scope. When using the concept of co-ordination, I do not refer to a single center where power is centralized and co-ordination is *done*. As Callon (1984, p. 224) observes in a study of scientific knowledge and the role of non-humans, the continuous displacements of actors draw out the ways in which power relations can shift when the equilibrium is modified, benefiting certain actors more than others. I turn to the co-ordination of financial intelligence in order to view how the negotiation of political stakes and the reconfiguration of power relations may take place in practice.

Materiality matters

Second, this research enquires into the materiality of transnational practice. Transnational financial intelligence exists in the materiality of daily practices that form the basis of intelligence sharing and political and geopolitical security operations. Mol (2002, p. 27) emphasizes the importance of materiality and non-humans in her ethnography of atherosclerosis, writing that "however important feelings and interpretations may be, they are not alone in making up what life is all about. Day-to-day reality, the life we live, is also a fleshy affair. A matter of chairs and tables, food and air, machines and blood". Including materiality echoes a broader shift prevalent in thinking in STS (Callon, 1984; Latour, 1987, 1999a, 2007b; Stengers, 2000), which has increasingly emphasized the significance of practice and the materiality and (inter)mediation of non-humans. Human worlds are not merely 'social' but take place and exist in the materiality of practice, where a multitude of things – both alive and not – affect the state of affairs (see, e.g., Callon, 1984; Laet & Mol, 2000; Latour, 2017, 2018, 2021; Law, 1986; Star, 1990).

For example, in an early STS study, Callon (1984) investigated the domestication of scallops in France and the manner in which these were being harvested for commercial purposes. Callon (ibid.) concluded that not only the fishers and researchers played an important role, but the non-human scallops exhibited considerable agency, too, as they resisted certain kinds of domestication. By including non-human actors, Callon (ibid., p. 223) demonstrates that knowledges are produced through steps of *translation* that emphasize "the continuity of the displacements and transformations which occur in this story: displacements of goals and interests, and also, displacements of devices, human beings, larvae and inscriptions". Callon's inclusion of non-human actors, such as documents, technologies and animals, adds an entirely new layer to ethnographic inquiry.

In a similar vein, Latour (1999) accompanied a group of botanists studying the Amazon to determine whether a part of the forest was expanding or retreating. He describes various stages of translating scientific knowledge on the forest, entailing what he calls a "chain of translation" through which academic knowledge is based on continuously gathering, assembling, and reassembling information (ibid., pp. 24–79). From the collection and ordering of parts of the forest into labeled "evidence", to the interpretation of this evidence and its publication in an academic journal, Latour (ibid., p. 74) demonstrates that "each stage is matter for what follows and form for what precedes it". As Levi and Valverde (2008) summarize:

> [Translation] refers to all the moves and links that make up a network – the intellectual moves that facilitate moving the knowledge process along as well as the physical movement of people and things from one place to another. Analysts are to follow the translations, adaptations, alliances, and controversies that occur (Levi & Valverde, 2008, p. 810).

This approach offers novel analytical tools with respect to the study of the production of transnational financial intelligence, in a similar fashion as De Goede (2018) followed a single transaction through the 'chain of security'. In addition to the perspectives of professionals and their daily understandings, dilemmas, and challenges, the translations and networks involved non-human actors, like the suspicious transaction itself, software programs, artificial intelligence, pre-established (international) typologies, policy documents, and red flag systems. This dissertation takes into account the material contexts in which security threats, such as terrorism financing, are constructed and brought into being. Also mundane elements such as "diagrams, computer networks, scientific data, and even the specific forms that need filling in" are taken as essential in the construction and understanding of security fields (Huysmans, 2006, p. 8).

Furthermore, this research argues that including the materiality is key to understand *transnational* practices of exchanging financial intelligence. There is a growing IR scholarship on how material objects connect internationally (e.g., Leander 2015b, 2021; Salter, 2015, 2016). The so-called 'material turn' (Salter, 2015) has inspired study of the international mediation of even mundane things, such as garbage (Acuto, 2015), tanks (Shapiro, 2015), and bicycles (Löwenheim, 2015). In security studies, the mediation of technologies has been a focus, such as body scanners at airports (Bellanova & Fuster, 2013) and border walls (Pallister-Wilkins, 2016). In a similar vein, this dissertation includes materiality to understand the everyday operations of FIUs and their transnational exchange of financial intelligence, focusing on the role of reports, software programs, documents, minutes, standardizations, XML formats, statistics, numbers and mundane and easily overlooked things, such as meeting rooms. Following Huysmans (2011, p. 371), it includes the seemingly banal "little security nothings". To understand formations and processes of grand geographical scope and scale, I argue, we need to focus on the material, small and often technocratic practices at the basis of international financial intelligence exchange and geopolitical co-ordination – specifically, by focusing on certain vantage points.

Vantage points

Third, this dissertation adopts different vantage points in order to unpack transnational processes in practice. Given that 166 FIUs engage in countless bilateral and multilateral interactions, it is difficult to decide which (material) practices provide a 'good' perspective to understand transnational processes. On what basis should certain practices be selected, and how should the salient practices be studied? A vantage point, according to the Oxford English dictionary, is "(a) a place affording a good view or prospect" and "(b) the point from which a scene is viewed" (Brown, 1993, p. 3,546). This research advances the concept of vantage points as an analytical and methodological 'tool' providing an advantageous point of view on the co-ordination of transnational processes in practice, in which actors encounter one another and political negotiations

and the reconfiguration of power relations takes place. I use vantage point instead of places, sites, or locations, because from a particular vantage one can view and observe geographically scattered practices, rather than merely a demarcated space. This section discusses how I selected my vantage points and the methodological and conceptual advantages that the use of vantage points entails for the study of transnational processes in practice.

The notion of vantage point is well known and often considered in the context of photography. In that field, determining the vantage point is a continuous consideration, because the particular viewpoint from which a photo is taken affects the resulting image and, in effect, what the viewer observes. Photographer Vijayakumar writes that:

> The position from where you capture an image is the vantage point in photography. In simple words, "It is the angle of image capture." When you photograph the same scene from different positions, the size and position of various elements in the scene also change. Some elements will look bigger, and others will look smaller when you change the angle of view for the same scene (Vijayakumar 2022).

Figure 1.2 presents an example from Vijayakumar (2022) of two vantage points on a forest: an eye-level view and an aerial view. Each reveals particular features of the same materiality. Other vantage points that are used in photography are a low vantage point (viewing upwards), a high vantage point (viewing downwards), a close-up (revealing details), long shots (drawing one element out) and direct shots (placing a subject in the middle) (ibid.; see also Mendoza, 2016). Each of these vantage points changes the size, composition, and position of elements, making some potentially larger, smaller, or positioned differently in the eyes of the viewer.

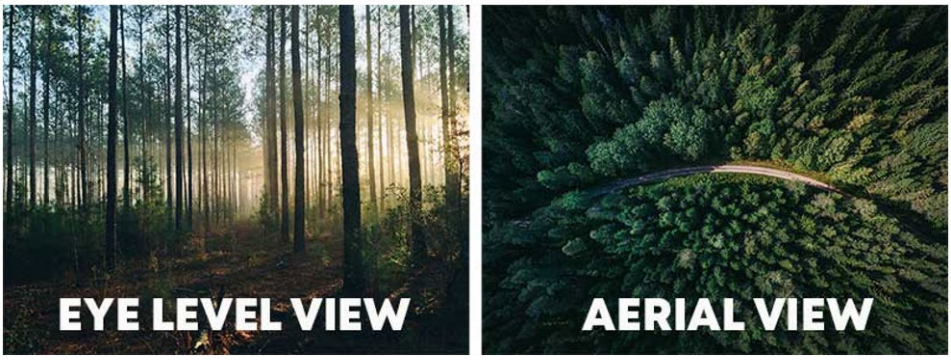


FIGURE 1.2: Different vantage points on a forest. Source: Vijayakumar (2022).

The discussion of vantage points in photography is interesting for our purposes, as it provokes thinking about the point of view that the researcher adopts. The chosen vantage point determines to a considerable extent what the viewer can observe, which elements are dominant and which recede to the background, and their respective and relative sizes. Moreover, the reference to photography emphasizes the decisive role of the *dynamic* positioning of the researcher in relation to the topic of interest and of the ultimate vantage point *selected* for the way in which transnational processes are captured.

In the study of transnational processes using qualitative or ethnographic methods, the possible viewpoints are seemingly endless. Where should one stand and focus? I found that available qualitative methodological approaches were not necessarily accustomed to studying transnational processes. One approach is to choose a particular location or topic, which is often called a 'case study' (Swanborn, 2012), focusing on a demarcated fieldwork site and gathering richly detailed empirical data to reflect on large processes. Or, a multi-sited ethnography might be conducted in which several fieldwork sites are chosen (Marcus, 1995), making it possible to reflect comparatively on broader processes. Another possible approach is to take global processes as the central unit of analysis, such as the earlier discussed 'scapes' proposed by Appadurai (1996), and ethnographically study how these play out locally.

However, as Tsing (2005) points out, ethnographic inquiries into global processes tend to get trapped in a binary framework between the global and the local:

> Many ethnographers find ourselves with data about how a few people somewhere react, resist, translate, consume, and from here it is an easy step to invoke distinctions between local reactions and global forces, local consumption and global circulation, local resistance and global structures of capitalism, local translations and the global imagination (Tsing, 2005, p. 58).

Tsing (ibid., p. 1) warns of the theoretical trap of choosing between "the universal and the culturally specific". I experienced this pitfall myself in my previous research on Indian stockbrokers (Lagerwaard, 2015), in which I argued on the basis of a case study of the Mumbai stock market that brokers 'negotiate' global finance. In hindsight, I can discern a tension between my point of view on the stock market of Mumbai and the conceptual conclusions I drew by referring to a grand process (global finance) that serves as an abstract framework in which to situate my findings. The stockbrokers, in this viewpoint, merely "react, resist, translate, consume" (Tsing, 2005, p. 58).

While actor-network theory provides tools to move beyond the binary between the global and the local and study the unbounded movement of actors in practice (Michael, 2017), the generally proposed strategy – to 'follow' the actor – remains rather

ambiguous, in particular when studying large-scale processes. Latour (2007, p. 12) writes, "you have 'to follow the actors themselves', that is try to catch up with their often wild innovations in order to learn from them what the collective existence has become in their hands". Yet, where should one start to follow an actor? What actor, for how long, in what direction, and where does one stop? As the reference to photography demonstrates, *it matters* where one begins, and what mediating actors are pursued and how far. Especially when studying (material) transnational processes of potentially enormous scope and scale, the plethora of actors that one can start to follow can be overwhelming.

A 'good' vantage point, I argue, is determined by the researcher's dynamic positioning when selecting it. Drawing on the work on friction by Tsing (2005, p. 5), I propose to actively search, recognize, and study the *encounters* between (non-human) actors across distance and difference, where the friction of the encounter produces metaphorical "heat and light" that make the co-ordination visible and amenable to study. Tsing (ibid., p. 4) proposes moving beyond the dichotomy between – I paraphrase – the general global and the particular local by studying 'friction', by which she refers to "the awkward, unequal, unstable, and creative qualities of interconnection across difference" – or, more abstractly, the "grip of worldly encounter" (ibid., p. 1). In her study of deforestation in Indonesia, Tsing (2005) finds that friction emerges when different actors from different places, each with their own aspirations, meet: forest dwellers, (Western) nature activists, Japanese trading companies, and Indonesian politicians – all with their own conceptions of deforestation that collide. Importantly, these interconnections and encounters are *productive*, according to Tsing (ibid.), in that they lead to new arrangements power:

> A study of global connections shows the grip of encounter: friction. A wheel turns because of its encounter with the surface of the road; spinning in the air it goes nowhere. Rubbing two sticks together produces heat and light; one stick alone is just a stick. As a metaphorical image, friction reminds us that heterogeneous and unequal encounters can lead to new arrangements of culture and power (Tsing, 2005, p. 5).

It is these moments of friction and their importance for producing "new arrangements of culture and power" (ibid.), that I take to be essential in selecting the focus of this dissertation. These moments have sufficient visibility to guide the research and researcher, while also constituting interesting contexts for study, as new arrangements of power are (re)produced here. To some extent, the notion of friction and encountering global connections resembles the debate on controversies in STS (De Vries, 2016; Latour, 1987; Schouten, 2014). Here, a controversy is assumed to reveal associations

that were first invisible, due to their stability and background role, but become visible and the subject of debate due to controversy, and therefore amenable to study. However, when studying global connections, the actors and assemblages are not confined to a demarcated space where the controversy takes place, such in a laboratory (Latour, 1987), but are potentially geographically scattered and connected around the globe.

I propose the use of different vantage points that provide views on encounters between security practitioners that generate so much 'heat and light' that they become visible, and therefore make possible to study how transnational processes are co-ordinated in the materiality of practice. Such friction between different actors serves as the *leitmotif* for selection of ad*vantage*ous viewpoints, as friction may draw out where co-ordination becomes explicit, transparent, and visible, and therefore "opens the possibility of an ethnographic account of global interconnection" (Tsing, 2005, p. 6). This friction does not have to be situated in one place, but can take place at many dispersed sites and locations, including digitally. The positioning and selection of viewpoints determines which elements become prominent, and which recede to the background. A number of questions can guide selection of relevant vantage points: Where do actors encounter one another? Where are practices secretive, delicate, tense, and perhaps controversial? What issues, topics, or activities seem to be sensitive? Where do you, as a researcher, sense perhaps intuitively, that things are 'mattering', that people are worried, anxious, happy, or excited? Where are the conflicts, disagreements, negotiations, and collaborations the fiercest and most intensely passionate? Where do (transnational) things and affairs rub together?

The use of different vantage points contributes to the study of transnational processes both methodologically and conceptually. Using different vantage points enables the researcher to conduct qualitative, flexible, and iterative research of transnational processes, without falling back on the global-local binary, on frameworks such as global finance, or on other self-explanatory ideas, such as capitalism, neoliberalism, and postcolonialism. Methodologically, using vantage points enables the researcher to select, through the initial iterative tracing of certain actors, a favorable viewpoint from which to observe the co-ordination of transnational processes in practice. As such, the research can obtain focus, rigorously use (mixed) qualitative methods, and pursue the object to the point where "data saturation" is reached – when new findings increasingly reaffirm old findings and new insights become scarce (Bryman, 2008, p. 412). Use of vantage points, therefore, enables in-depth qualitative empirical research on large-scale processes yet to 'break free' of a (multi-sited) demarcated fieldwork location or 'case study' (Swanborn, 2012). Different vantage points enable the researcher to shine different light on the main research question, each drawing out some elements while making others potentially smaller or positioned differently, in the eyes of the viewer.

Conceptually, the use of vantage points enables the researcher to focus on the moments that matter, where political stakes and reconfigurations of power take place,

in practice, and where the movement of things is most productive. Instead of following whatever to wherever, with vantage points it becomes possible to *empirically* focus and observe how power and politics play out in the materiality of specific practices of co-ordination. In particular, when studying geopolitics, power is often viewed as an instrumental force whereby countries engage in contestations through transnational institutions. Studying vantage points means investigating the shifting and translating power relations in which actors might clash, entwine, conflict, or collaborate in practice (see Callon, 1984). Focusing on practice makes it possible to view what Mol (1999, p. 83) calls an "ontological politics" where "realities may clash at some points, [and] elsewhere the various performances of an object may *collaborate* and even *depend on* one another" (emphasis in original). By studying how political stakes and the reconfiguration of power play out in practice, vantage points enable the researcher to cut through the theoretical hierarchies that are often implicitly assumed in disciplines such as IR and international political economy.

By adopting different vantage points, this dissertation aims to provide distinct yet overlapping views on the main research question. Taken together, the different vantage points contribute to a more substantial understanding of how FIUs co-ordinate their operations transnationally and exchange financial intelligence across distance and difference. The empirical sections – four in total – each adopt a different vantage point. Chapter 3 adopts as its vantage point *FIU-the Netherlands*, where the financial intelligence that is exchanged is produced through the core practices of collecting, analyzing, and disseminating transaction information. Chapter 4 adopts as its vantage point the *EU FIUs Platform*, a European Commission Expert Group that includes 30 FIUs in which shared understandings of data exchange are produced. Chapter 5 takes the *numbering practices* of FIUs as its vantage point; these practices provide FIUs with a depoliticized technocratic vocabulary with which to co-ordinate cross-border operations. Chapter 6 adopts *circuits of trust* as its vantage point, to reveal how informal relationships between FIUs are built and maintained and serve as a basis for the exchange of intelligence. The next section introduces these vantage points in greater detail, provides an outline of the dissertation, and introduces its sub-questions.

1.5 Research questions and outline of the thesis

This section offers an outline of the dissertation, alluding to the different vantage points and discussing the various sub-questions. Following this introduction chapter, Chapter 2 elaborates on the research methodology, discussing data collection strategies and data handling protocols. Each vantage point led to a specific selection of empirical data, for which various processes of gaining access had to be undertaken. This required considerable effort and patience, given the secrecy that is part and parcel of this

security field. Chapter 2 thus describes how I gained access to conduct interviews at the Netherlands' FIU, at European FIUs, and with a range of other practitioners, such as bank employees. Chapter 2 also discusses the methods of data collection and analysis; specifically, semi-structured interviews, participant observation, and document analysis. Finally, the chapter describes how I handled, stored, and protected the data and the choices I made concerning ethics, anonymity, and data dissemination.

The vantage point adopted in Chapter 3 is that of the FIU of the Netherlands. National FIUs produce financial intelligence in different ways, rendering the exchange of such intelligence across distance and difference more complex. Chapter 3, therefore, begins by describing the core practices of FIUs and how transaction information is – secretly or openly – transformed into financial intelligence. Financial intelligence includes privacy-sensitive information, which is subject to confidentiality and caution. To unpack how financial intelligence is produced, the chapter examines one FIU, in order to gain a fine-grained understanding of the production of intelligence and the core tasks that FIUs perform. It deploys novel methods to "encircle" the secrecy aspect (Bosma et al., 2019, p. 14) and asks how the FIU, in practice, fulfils its core tasks of collecting, analyzing, and disseminating financial and related information.

Chapter 4 adopts the EU FIUs Platform as its vantage point. This European Commission Expert Group plays a crucial role in the coordination of intelligence exchange in the EU. Its 30 member FIUs, as well as the European Commission, meet physically several times per year in Brussels. Within the platform, different versions of financial intelligence encounter one another, each having different aspirations concerning the means of exchange, the nature of financial intelligence, and the legal obligations of intelligence exchange. The chapter asks how geographically dispersed FIUs produce and navigate common understandings of data sharing. By 'flattening the international', the chapter explores the importance of materiality to understand the coordination of transnational financial intelligence exchange in practice, such as the role of meeting minutes, timetables, and even meeting rooms.

Chapter 5 adopts as its vantage point the numbering practices of FIUs. FIUs generate massive amounts of quantitative data on security issues, such as terrorist financing and money laundering. However, FIUs apply different practices of numbering and statistics, which generates certain tensions and debates between FIUs and intergovernmental organizations. This chapter zooms in on these numbering practices, in particular, those on terrorist financing, and inquires as to how FIUs coordinate their operations through disparate knowledge practices of numbering terrorist financing. The chapter demonstrates that a vantage point does not have to be a national or intergovernmental organization or location. Rather, certain practices that are geographically scattered can provide a favorable empirical viewpoint to learn about how FIUs work across distance and difference. The chapter shows that numbering practices provide a depoliticized technocratic vocabulary, through which FIUs can coordinate their operations.

Chapter 6, finally, adopts circuits of trust as its vantage point. Trust – or distrust – is generated through circuits of webinars, conferences, and workshops, in which actors from around the globe meet and build informal relationships. Through these circuits of trust, practitioners encounter one another and engage in a politics of trust that makes the sharing of sensitive financial intelligence either possible or out of the question. This chapter examines how formal and informal political practices and circuits of trust render sensitive financial data and transactions internationally shareable. Specifically, three practices are examined: the use of trust circuits to navigate a 'legal grey zone' in which FIU data are shared; the way trust circuits make intelligence sharing possible (or not); and how the implicit notions of trustworthiness and untrustworthiness lead to inclusion and exclusion.

Chapter 7 closes the dissertation, returning to the main research question and connecting the different vantage points adopted in the empirical chapters. A general conclusion is that it is the relatively informal nature of international agreements, combined with the autonomy of FIUs, that enables FIUs – through hard (coordinating) work – to share privacy-sensitive intelligence around the globe. Based on this conclusion, the chapter distills two areas recommended for further research. One line of further research is to unpack the question of how FIU intelligence is used further down the chain of financial security, and the other is to study the growing role of non-Western FIUs. Finally, the chapter raises questions on the societal consequences of financial intelligence and the operations of FIUs, particularly with regard to oversight, accountability, and proportionality. These issues arise throughout the dissertation, and merit further public and political attention. The conclusion will therefore be of interest not only to academics, but to politicians, policymakers, and practitioners as well.

TABLE 1.1: Research question and sub-questions. Source: Author.

Research question	**How do FIUs coordinate their operations transnationally and exchange financial intelligence across geographical distance and organizational difference?**	
Chapter	**Vantage point**	**Sub-question**
3	FIU-the Netherlands	How does the FIU fulfill the three core tasks of collecting, analyzing, and disseminating financial and related information in practice?
4	EU FIUs Platform	How do geographically dispersed FIUs produce and navigate common understandings of data sharing?
5	Numbering practices	How do FIUs coordinate their operations through disparate knowledge practices of numbering terrorist financing?
6	Circuits of trust	How do formal and informal political practices and circuits of trust render sensitive financial data and transactions internationally shareable?

2

Studying FIUs

2.1 Introduction

This research argues that to obtain in-depth knowledge of transnational processes, such as the exchange of financial intelligence by FIUs, we must turn to seemingly small everyday practices. Along similar lines, Tsing (2005, p. 6) suggests that "[a]bstract claims about the globe can be studied as they operate in the world". Because little is empirically known of FIU practices and the transnational exchange of intelligence, the current research commenced from the "context of discovery" (ibid., p. 16), implying that "the research process is largely *inductive* – that is, the researcher begins with concrete observations of the phenomenon itself and attempts to develop a more abstract description of or a theory about the phenomenon" (ibid., 17, emphasis in original). By moving back and forth between empirics and theory, I gradually and iteratively sharpened my research and recognized, distilled, and focused on the four vantage points already introduced.

In this process I relied, in particular, on qualitative methods, such as semi-structured interviews with professionals in FIUs and other security practitioners; participant observation at practitioners' conferences, workshops, and trainings; and analysis of documents, such as policy reports, meeting minutes, and legislation (Table 2.1). The qualitative fieldwork was conducted from 2016 to 2020, initially at a gradual pace, and then picking up speed as my network of practitioners expanded. In time, I gathered data using strategies and methods such as snowball sampling (Bryman, 2008, pp. 184–185), "encircling secrecy" (Bosma et al., 2019, p. 14), participant observation

(Spradley, 1980), and the aforementioned semi-structured interviews (Bryman, 2008, pp. 438–439).

To study everyday practices, it was crucial to gain access to the field of financial intelligence. Early on, this proposition presented many uncertainties. It was unclear whether I would receive permission from FIUs to conduct interviews and whether I would gain access to relevant information as well as to practitioner conferences and workshops. It was even unclear what the best starting point for the research might be. This recalls Law's (2004, p. 2) slightly provocative question: "[If] the world is vague, diffuse or unspecific, slippery, emotional, ephemeral, elusive or indistinct, changes like a kaleidoscope, or doesn't really have much of a pattern at all, then where does this leave social science?" To attune to this challenging context, I relied on the grounded theory approach. This meant constantly switching back and forth between empirics and theory, gradually selecting my vantage points and sharpening my research focus, questions, and conclusions (on grounded theory, see Glaser & Holton, 2004; Glaser & Strauss, 1967).

To be transparent and explicit about my choice of methods and research strategy, the sections below present a linear narrative from the beginning of my PhD project. Section 2.2 thus begins with my initial research question, which deviates somewhat from the current one (on this, see Cheng, 2018), and explains how I gained access to this security field in which secrecy is part and parcel of everyday operations. Section 2.3 elaborates on how the vantage points emerged during the fieldwork, the methods I used, and the data I gathered. Section 2.4 reflects on ethical deliberations and secure data handling, which are two particularly important topics to consider when studying such a sensitive and secretive field as financial intelligence. Finally, Section 2.5 offers conclusions.

2.2 Gaining access

In order to study practice, it was vital for me to gain access to the secretive field of financial intelligence, in which many processes and things – such as the actual financial transactions – are classified as secret and not accessible to researchers. This section discusses how I gained access to practitioners with whom I had no prior acquaintance. My initial research question was somewhat different from the central question posed in this dissertation and applied a slightly different scope. I initially asked, *How do European financial intelligence actors, and in particular those working at a financial intelligence unit (FIU), enact financial intelligence?* I initially chose to study European financial intelligence actors because I was unsure about the scope and scale that my research would – also pragmatically – permit. Furthermore, I focused on financial intelligence actors more broadly instead of only FIUs because I was unsure whether I would manage to gain access to FIUs and interview practitioners within them. At the

time, I had written an analysis of the annual reports of EU FIUs (Lagerwaard, 2018). Yet, I still lacked a network in the field of financial intelligence, and I did not personally know any practitioners in any way connected to an FIU, let alone working at one.

One thing that helped me to gain the needed access is that this research was conducted as part of the broader FOLLOW project: "Following the Money from Transaction to Trial".[9] FOLLOW aims to study how unusual or suspicious financial transactions travel from one security domain to another. Because FOLLOW encompass various domains, such as banks, FIUs, and courts, I conducted my research in close collaboration with other team members via collaborative semi-structured interviews, jointly visiting conferences and workshops, and sharing data and expertise. Yet, the bulk of the data used in this dissertation derives from fieldwork conducted specifically for my PhD research (see Table 2.1).

Working as part of a broader project had the advantage that as a group we could build a public profile, which from the start enjoyed some legitimacy, because of FOLLOW's status as a European Research Council (ERC)-funded project. Furthermore, the project's general purpose resonated well with practitioners, as it emphasized the daily dilemmas and challenges that they themselves experienced. The opening conference of the FOLLOW project provided my first introduction to practitioners in the field, enabling me to get started building my own network. This conference included academics, lawyers, practitioners from banks, and other professionals in some way connected to the field of financial intelligence. At the conference, I was able to meet and build rapport with several bankers, whose inputs later proved valuable, particularly for the FOLLOW project on banks (on rapport, see Bryman, 2008, p. 201; Rutten, 2007). In fact, many of the initial interviews I conducted for my research were not with FIU employees, but with other practitioners, such as bankers, to whom I could ask questions about the role of FIUs. This was a suitable first step, as it allowed me to explore and 'map' the field of FIUs from a distance. I used this preliminary data to understand the norms, values, and vocabularies of the sector (Gusterson, 2008).

Another important opportunity connected to the FOLLOW project, though separate to some extent, was a collaboration with Dr. Mara Wesseling, who conducted research for the Dutch Ministry of Justice and Security's Research and Documentation Centre (known by the acronym *WODC*, from the Dutch name).[10] That project mapped the actors involved in combatting terrorist financing in the Netherlands, including the role of the FIU. In collaboration with this project, I conducted my first interviews with FIU employees, and this therefore constituted my first direct access to the field I aimed to study. From these first connections, I generated my own relations with the Netherlands'

9 This project received funding from the European Research Council (ERC) under the EU Horizon 2020 research and innovation programme (grant no. ERC-2015-CoG 682317).

10 In Dutch this is organisation is called the Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC).

FIU and officially requested permission to conduct research at the organization. After a lengthy process, this permission was granted, yet with substantial limitations because the actual analyses of financial transactions by the FIU would remain off limits, unless I agreed to an extensive process of vetting and screening, which would have been overly time consuming and posed possible limitations to what I would have been allowed to publish. Chapter 3 sets out how I resolved the difficulty of secrecy in the field of security research, using the "encircling secrecy" method developed by Bosma, De Goede, and Pallister-Wilkins (2019, p. 3). In brief, the notion of encircling secrecy shifts the focus away from the 'kernel' of the secret, to find ways to understand the "mundane lifeworlds of security practices and practitioners" (ibid., p. 14). As part of the encircle secrecy method, I followed an online e-course designed for FIU analysts, which permitted me a glance behind the scenes, though in a generic sense. The FIU did grant me access to conduct several interviews with employees working on different topics. These offered enormous insight into the inner operations of the FIU.

Simultaneously, I applied another strategy to gain access to the field; that is, participant observation (Bryman, 2008, pp. 402–403; Eriksen, 2010, pp. 25–26; Spradley, 1980). I visited practitioner conferences and workshops, both to participate and observe as well as to build a network in the field and find new connections and interviewees. To give an example, I went to a week-long conference called the Cambridge Symposium on Economic Crime in 2018. This is a key venue for practitioners to make contacts and become part of transnational networks. At the symposium, I participated in workshops, joined presentations, and perhaps most important, joined in diners, lunches, and end-of-day cocktails. I conducted several interviews while there, observed (in some cases intimate) connections between practitioners, and learned extensively about topics that mattered in the field of financial intelligence. Through this conference I gained insights into processes that extend beyond individual FIUs and the EU, thus providing input for, in particular, chapters 5 and 6. Similarly, I visited conferences with fellow team members from the FOLLOW project, and we organized our own events, which many key stakeholders visited, such as the closing event for the aforementioned ministerial research.

The participant observation and building of my network, together, culminated into what the methodological literature often terms "snowball sampling" (Bryman, 2008, pp. 184–185), whereby new points of access and relations result in further access. For instance, in collaboration with Dr. Rocco Bellanova, I conducted interviews that – through our combined networks with practitioners – resulted in a connection to the EU FIUs Platform. This led to the opportunity to introduce our research via a one-pager that was discussed at one of its meetings and circulated online. The platform is important because it is the key location where European FIUs discuss the international exchange of financial intelligence. The introduction of my project at an official EU FIUs Platform meeting – also becoming part of the minutes that I later meticulously studied

– made it possible for me to approach FIUs across Europe with requests for interviews on international cooperation. Some FIUs collaborated with enthusiasm, while others were more reluctant and preferred, for example, answering my questions via e-mail. I conducted several interviews via Skype (Zoom or Teams was not yet common practice). A few of these proved crucial for the research, providing vital information, in particular, for Chapter 5, on the numbering practices of terrorist financing, and for Chapter 6, on the role of trust in transnational intelligence sharing. I studied the workings of the EU FIUs Platform itself primarily by precisely reading the minutes of platform meetings. These were quite technical but also surprisingly open and clear about the discussions that took place. As such, I combined documents such as minutes and policy documents with interviews and participant observation, selecting and focusing on vantage points and gradually arriving at the point of data saturation – when similar findings reappear and new findings become increasingly sparse (Bryman, 2008, p. 412). Fortunately, I had conducted several key interviews just before the COVID-19 pandemic erupted.

2.3 Vantage points: Methods and data

This section explains how the vantage points adopted in this research were studied; that is, the methods and data that provided me an advantageous point of view on transnational financial intelligence processes. As observed in Section 1.4, using vantage points enabled me, in my role as researcher, to break free from a demarcated research location, while still applying a flexible, iterative research process supported by qualitative methods, to gather rich empirical data on transnational processes. By focusing on the encounter of global connections and those moments where arrangements of power were produced or reproduced, the transnational became visible and amenable to study. Furthermore, I applied grounded theory, moving back and forth between theory and empirics. My vantage points were not selected up front as part of the research design; rather, these emerged through the tracing of certain actors that metaphorically radiated "heat and light" (Tsing, 2005, p. 5). I did not search for, identify, and select my vantage points one after the other, nor did I necessarily finish studying one before turning to the next. Rather, adopting the vantage points had the benefit of gradually focusing the research, while simultaneously keeping several pursuits open that gained form in parallel.

This flexible research approach meant that the methods and data collection did not follow a linear path, but developed gradually and accumulated in tandem with the vantage points. An advantage was that data gathered could be useful at several points in the research, in different ways, and provide specific empirical evidence for the vantage points. This process, however, posed a challenge regarding the structuring of the data, as will be discussed below. Taken together, the primary research data were gathered using the three aforementioned methods: semi-structured interviews, participant observation,

and document analysis (see Table 2.1). However, due to the flexible and parallel research approach, each of the empirical chapters draws on different combinations of these.

Fairly quickly, the Netherlands' FIU emerged as an interesting vantage point to adopt, not only because of its technologically advanced practices, but also because it is within an FIU that the intelligence is produced that is eventually exchanged with foreign FIUs. FIU-the Netherlands is an active member of the EU FIUs Platform. Furthermore, at the time of this writing the chair of the Egmont Group was held by the head of FIU-the Netherlands. To study the internal operations of this FIU, I followed an e-learning course on operational analysis and conducted semi-structured interviews with FIU practitioners, including five practitioners from FIU-the Netherlands and eight from FIUs in other EU countries. The e-learning course enabled me to experience the work of an FIU analyst myself. It consisted of 15 sessions, offered for FIU analysts by the Basil Institute on Governance. The course provided me a behind the scenes impression of how FIUs analyze financial information and send intelligence to security partners further down the chain, by doing so – fictionally – myself. The semi-structured interviews gave me the opportunity to enquire into the experiences and dilemmas of FIUs in practice, again offering a glance behind the scenes. In addition, I conducted document analysis, including a study of the annual reports of FIU-the Netherlands. This provided a longitudinal overview of the quantities of reports that the FIU handled.

The second vantage point inductively emerged when tracing intelligence exchanges within the EU, which is a challenging process given the diverse nature of the 31 FIUs involved. I recognized a relatively unknown EU Commission Expert Group that was crucial for the coordination of intelligence exchange and proved a favorable second vantage point: the *EU FIUs Platform*. To adopt this point of view, I used primarily document research and semi-structured interviews. In particular, I drew on the minutes of meetings of the EU FIUs Platform. To my own surprise, these are recorded and publicly accessible online. By meticulously analyzing these minutes from 2014 to 2019, I learned about the history and development of FIU cooperation and, perhaps more importantly, about the most prominent and challenging debates among FIUs during the fieldwork period. In other words, I could read with the FIUs about the debates they were having, the points on which they conflicted, agreed, or needed to conduct further discussion. In addition, structured interviews and semi-structured interviews with representatives of FIUs and other practitioners, enabled me to situate and contextualize the information from the annual reports and minutes.

My research pointed increasingly to the importance of statistics and numbers on money laundering and terrorist financing. Adopting as a vantage point the *numbering practices* of FIUs provided insights into the role of these practices in providing a depoliticized technocratic vocabulary that enabled FIUs to coordinate their transnational operations. To study the disparate practices of numbering terrorist financing, I conducted semi-structured interviews and used documents from the EU FIUs Platform, Europol,

the Egmont Group, and the FATF. The interviewees I managed to approach via the EU FIUs Platform proved a valuable source for gathering data about the different ways in which FIUs construct terrorist financing and the practices they deploy. In addition to the semi-structured interviews, I gained insight through some structured interviews. For these latter, I sent FIUs a questionnaire asking about their numbering practices. Many of these were completed and returned to me via e-mail, and I followed up with additional questions. Furthermore, I used documents from Europol and the EU FIUs Platform to unpack a controversy between these two organizations about the lack of harmonization of numbering practices.

The final vantage point, *circuits of trust*, emerged especially during my fieldwork presence at conferences, webinars, and workshops. Because trust is generated in particular through *informal* practices, these venues proved fruitful for observing how trust – or the lack thereof – influences the sharing of financial intelligence. For instance, observing warm embraces between FIU practitioners during an informal cocktail party helped me to recognize how important it is to get to know one another, to meet, have drinks, and in the words of one informant, "to look someone in the eye" in order to gain their trust (Former HoFIU, September 6, 2018). However, the importance of trust in coordinating the politics of the transnational exchange of intelligence also emanated from my document research and semi-structured interviews. From these, I learned that trust is semi-institutionalized, often appearing in nonbinding regulations, and that it is crucial in the daily practice of intelligence sharing.

Data

Taken together, I engaged with a total of 37 practitioners and conducted 29 interview sessions, of which 16 sessions were recorded. The interviews were unstructured, structured, or semi-structured, though most were the last. Unstructured interviews refer to informal engagements ranging from in-depth conversations to unexpected impromptu interviews, for instance, at conferences. The structured interviews reflect to some extent an interview guide, which included open questions that I sent to FIUs that indicated a preference not to participate in an interview either face-to-face or via computer. Often, I followed these up with requests for additional clarification via e-mail. The semi-structured interviews relied on an interview guide (Bryman, 2008, p. 695) designed to steer the conversation while providing ample space to flexibly touch on new and unexpected topics that might surface during an interview. The numbers of the various types of interviews, as displayed in Table 2.1, distinguish between *practitioners* and *sessions*, because some interviews involved several interviewees simultaneously (in one session), while others entailed double interviews of a single subject (counting as one practitioner).

The participant observations included fieldtrips, conferences, and workshops; social media interactions; and the e-course. I conducted two fieldtrips, to Brussels and to

London. These were primarily to gather data during planned interviews, but in practice they generated insights – both formal and informal – into how, for instance, security actors such as law enforcement use intelligence on terrorist financing. Conferences such as the Cambridge conference were other important fieldwork sites (see Table 2.1). During these events, I gathered notes on, for instance, new 'hot topics' in the field, the dilemmas that practitioners experienced and shared, and also the mundane and everyday relations and engagement between practitioners. In addition, I engaged with practitioners in the field by using social media, such as LinkedIn, to build and, especially, maintain a network of practitioners who were in some way involved in the broader field of financial surveillance. FIUs are surprisingly absent from social media, but practitioners working in the financial dimension of financial surveillance, such as bankers, are active.

The document analysis, finally, included a wide range of documents, such as annual reports from FIUs, documents from the FATF and the Egmont Group, legal and quasi-legal documents, and the aforementioned minutes of the meetings of the EU FIUs Platform. Between 2009 and 2014, I conducted an analysis of the annual reports of 10 European FIUs. That resulted in a working paper, with the main conclusion being that FIU statistics – and thus operations – are difficult to compare (Lagerwaard, 2018, p. 19). I studied documents from the FATF and the Egmont Group in an effort to grasp the foundation of transnational FIU cooperation, as translated into regional legal frameworks – such as the Sixth EU Directive on Anti-Money Laundering and Countering the Financing of Terrorism (6AMLD) – and national legal frameworks – such as the Netherlands' Anti-Money Laundering and Anti-Terrorist Financing Act (known by the acronym *Wwft*, from the Dutch name). I studied the minutes of the EU FIUs Platform from the 23rd meeting in November 2014 to the 39th meeting in March 2019. In addition, I examined annex documents, as well as reports drafted on behalf of the EU FIUs Platform, such as the extensive 'mapping exercise' it carried out in 2016 (EU FIUs Platform, 2016).

To analyze the data, I used various strategies. For the participant observation, I recorded fieldnotes. These ranged from brief observations only a page in length, to substantial reports on, for instance, the Cambridge conference and the e-learning course. For the document research, I applied systematic focused reading strategies, from note taking in Adobe Acrobat to the printing and binding of years of minutes of EU FIUs Platform meetings. To analyze the interviews, I used Atlas.ti, a software program that assists in the ordering, coding, and analysis of qualitative data – moving from open to selective codes and creating meta-categories in the process (Bryman, 2008, p. 543; Glaser & Holton, 2004). I labelled the 29 transcripts of the sessions inductively, arriving at 143 codes grouped into 14 meta-categories. Atlas.ti enabled me to structure the rather messy research data coherently and analyze it in the coding process, in so doing, generating many of the core arguments of the empirical chapters.

TABLE 2.1: Methods and sources of primary research data

Method	Practice		
Interviews	Interviews: • 37 practitioners • 29 sessions • 16 recorded See Annex A for details	Practitioners: • 17 FIUs • 7 law enforcement • 5 banks • 8 other	
Participant observation	• E-learning course for operational analysts: » 15 training sessions • Conferences and workshops: » Cambridge Symposium on Economic Crime » Chatham House, Illicit Financial Flows » 'Flying Money' conference in Amsterdam » Workshop with the Egmont Group » WODC closing conference • Fieldwork in London (2018) and Brussels (2019) » interviews and observations • Social media engagement		2017 2018 2018 2018 2019 2019 2018-2019 2016-present
Document analysis	Documents, among others: • Annual FIU reports (2009-2021) • Minutes of EU FIUs Platform (2014-2019) • Policy reports, e.g., from the FATF and the Egmont Group • Legislation, e.g., the Fifth EU Directive on Anti-Money Laundering and Countering the Financing of Terrorism, and the Netherlands' Anti-Money Laundering and Anti-Terrorist Financing Act (*Wwft*)		

2.4 Ethics, anonymity and data handling

The secrecy that is part and parcel of the field of financial intelligence raises important concerns, such as ethical questions, anonymity, and the secure treatment of research data. In preparation for this research, I received ethical clearance from the Amsterdam Institute for Social Science Research (AISSR). That clearance went beyond 'ticking boxes' of regulations; rather, it consisted of 10 open questions asking the researcher to contemplate important issues, such as concern for others, possible harmful research, informed consent, vulnerability of respondents, and anonymity. Furthermore, from its start, the FOLLOW project developed an ethics and research data protocol, including an ethical strategy regarding consent, risk, and conflicts of interest. FOLLOW has an independent ethics advisor, Dr. Anthony Amicelle, who has ample experience doing research in sensitive security fields. During the fieldwork period, we organized periodic meetings to discuss concerns and dilemmas with the ethics advisor, thus making ethics a continuous and recurrent contemplation during the research. This section addresses some of the main considerations that arose concerning ethics, anonymity, and data handling.

The respondents in the FOLLOW project, and in this research in particular, were not from a particularly vulnerable group in society. They resided in promising positions, many of which carried some weight in regard to responsibilities and accountability. To my knowledge, my informants were all highly educated. In this sense, the research involved 'studying up' instead of 'studying down' (Ho, 2009, 2012), as I engaged with practitioners who possessed authority and decision-making power to influence society. I affirm, therefore, in accordance with the FOLLOW ethics protocol, that no vulnerable adults were approached and no research participants received any form of payment from the researchers. Furthermore, I attest as prescribed by the FOLLOW protocol, that I was not interested in the operational details of ongoing investigations or in the content of financial transactions data. I was explicit in my research objectives and provided ample information on the project and its core questions before the interviews. Many respondents represented the executive branch of the state and, therefore, can be expected to bear a certain amount of responsibility in the information they chose to convey. During the interviews, respondents were capable of communicating effectively and of consciously navigating or tactfully avoiding sensitive topics and questions, if they wished to do so.

However, despite the research population not being particularly vulnerable and arguably in a position of power, the subjects did hold public and sometimes high-ranking positions and profiles. They were therefore relatively more exposed to the risk of public controversy. If their name was connected to a politically or otherwise sensitive topic, it could have serious individual and organizational consequences (see De Goede, 2020). I therefore chose to anonymize all respondents and the institutions they worked for, rather than only those respondents who requested anonymization. I also took precautions to guard against indirect recognition insofar as possible. In consultation with the ethics advisor the only exception to anonymization was FIU-the Netherlands, as this is the object of the case study presented in Chapter 3. Important details of the national context, such as the legal framework in which this FIU operates, the unique constellation of reporting entities and security actors, and the particular historical trajectory, make anonymization hard if not impossible to accomplish. It would also be undesirable because the ethical and political dilemmas and challenges faced by the FIU only make sense in its context. Nonetheless, I used no direct quotes in Chapter 3, in order to protect respondents' identities.

The data were stored securely on a laptop that was protected by a password and used only by myself. The research file containing the data were protected by Veracrypt, a virtually encrypted disk accessible only if it is first opened with another password. This password securely stored offline in the digital storage KeePass. This is a personal password storage utility that has to be opened with another password. Finally, to additionally secure the names of the respondents and organizations, I anonymized all of the interview transcripts, including the names of the organizations, including in the analyses software Atlas.ti. The transcripts were given a number that was also recorded

in a master document, kept as a separate file and only accessible using a password, which again was saved in KeePass. The research data was therefore inaccessible to anyone without the proper passwords; and even if access were illegally obtained, the data would still be anonymized.

If questions on the data are raised by academics or public actors, such as journalists, I will not reveal respondents' names or their companies. Neither will I disclose my transcripts or disclose descriptions of transcripts, memos, qualitative analyses, or any other such research material. In order to prevent respondents from being recognized, either directly or indirectly, I will share no data with any third parties whatsoever. This is not only to avoid the possibility of a breach of confidentiality, but also to prevent misinterpretation and misquoting of empirical data as a result of partial contextual knowledge. I realize that there is a tension here between research transparency, on the one hand, and the privacy and anonymity of respondents, on the other. To safeguard the internal validity of my research findings – and academic standards – both of my PhD supervisors can access my data without any restrictions, including the full names of people and organizations. In addition, if the data are questioned, the AISSR independent data steward can, upon request, receive full access to the data, including the names of people and organizations. Upon the steward's judgement, the case can be referred to the AISSR Integrity Committee, which would also receive full access to anonymized research data. Having these control mechanisms in place ensures high academic standards while, simultaneously, maintaining the absolute and guaranteed anonymity of respondents.

2.5 Conclusion

This chapter presented the methods used in this dissertation, the research strategy, and data handling protocols. I used three main methods – semi-structured interviews, participant observation, and document analysis – to study the daily practices of coordinating transnational financial intelligence. I gained access to the field by 'snowballing' and building a network among practitioners, benefiting from my collaboration with the FOLLOW project, of which this research was part. Starting from the context of discovery, I applied the grounded theory approach, moving back and forth between empirics and theory and sharpening the research focus, questions, and conclusion (Glaser & Strauss, 1967). In so doing, I gradually distilled the different vantage points of the empirical chapters. Chapter 3 turns to FIU-the Netherlands, a site of coordination that operates at various intersections. Chapter 4, then, studies the institutional vantage point of the EU FIUs Platform, in which 30 EU FIUs coordinate their operations and produce and navigate common understandings of data sharing. Chapter 5 takes disparate practices of numbering and statistics on the concept of terrorist financing as its vantage point,

examining how these enable FIUs to work across distance and difference. Chapter 6 turns to the circuits of trust and scattered physical yet fleeting moments of coordination, zooming in on the politics and relationships of trust (or distrust as the case may be). The conclusion, Chapter 7, draws together the findings of the different empirical chapters, revisiting the central research question on how FIUs coordinate their operations transnationally and exchange financial intelligence across geographical distance and organizational difference.

3

FIU-the Netherlands[11]

BOX 3.1 Vantage point: FIU-the Netherlands

This chapter adopts FIU-the Netherlands as its vantage point. This point of view is key to understand how FIUs work across distance and difference, because it provides insight into how the actual financial intelligence that is exchanged between FIUs is produced in practice. I found that each FIU produced financial intelligence in different ways, which made the international exchange of intelligence hard work, as the following chapters will demonstrate. To understand how this intelligence was produced in the first place, I focused on the three steps that all FIUs follow: *collecting* transaction information from commercial organizations such as banks, *analyzing* this information within the FIU, and *disseminating* the intelligence to law enforcement, the judiciary or foreign FIUs. Little is known about these internal operations, because the process of analyzing transaction information is shrouded in secrecy. To overcome the secrecy which is part and parcel of the field, this chapter uses the novel method of 'encircling secrecy', entailing a focus not on the 'kernel' of the secret but on the mundane practices of FIUs surrounding it (Bosma et al., 2019). The chapter concludes by raising questions regarding privacy, proportionality, and accountability, that will be further discussed in Chapter 6 and in the conclusion of the dissertation.

11 With some minor revisions, this chapter was previously published as Lagerwaard, P. (2023). Financiële surveillance en de rol van de FIU (FIU) in Nederland. *Beleid en Maatschappij*, (49)2, 128-153. It was translated from Dutch to English by Liz van Gerrevink-Genee. It has also been published in English as Lagerwaard, P. (2022). Financial Surveillance and the Role of the Financial Intelligence Unit (FIU) in the Netherlands. *Journal of Money Laundering Control*, (26)7, 63-84.

3.1 Introduction: FIU-the Netherlands

> There is a story behind every criminally-gained euro. A story that a banknote or bank transfer does not reveal but for some reason does end up at the FIU-the Netherlands (Akse, 2019, p. 6).

To mark its 25th anniversary, the financial intelligence unit of the Dutch police (henceforth, FIU-the Netherlands) published a book on the FIU's origins and core tasks (Akse, 2019). The book provides specific examples of the FIU's value in matters of security. It recounts the case of the woman who wanted to withdraw €100,000 in cash, to have – such was the suspicion – her ex-boyfriend murdered. Accordingly, the money was not paid out. Another example is the FIU's contribution to the high-profile investigation of the murder of Dutch politician Pim Fortuyn. Based on the FIU's financial data, the police were able to trace the whereabouts on the day of the murder of the man eventually convicted, Volkert van der Graaf. According to the jubilee book, "intelligence on reported transactions increasingly stakes a rightful place in investigation and prosecution.… Whether concerning the murder of Fortuyn, payment for a container of fruit with concealed parcels of cocaine, or healthcare fraud,… reported transactions play a crucial or supportive role in all these kinds of investigations" (ibid., p. 8).

During its now more than twenty-five years of existence, the Dutch FIU has grown to become the pivot of financial surveillance in the Netherlands. Coupled with the increasing digitization of payment services, as societies have transitioned from the use of coins and notes to digital transactions, a growing volume of financial transaction data has become available, from banks, but also from shops and service providers such as Western Union. These data provide a wealth of intelligence on citizens' spending behavior, and can provide insights into criminal activities. Commercial companies, particularly banks, that have access to transaction data are often seen as 'gatekeepers' of the financial system. According to the Anti-Money Laundering and Anti-Terrorist Financing Act of the Netherlands, these gatekeepers must monitor their customers for unusual, potentially criminal activities. At the time of this writing, banks in the Netherlands were estimated to have more than 12,000 employees whose primary task was to conduct customer screening, to monitor transfers of funds and transaction behavior of Dutch citizens, and to report unusual transactions to the FIU (Kamphuis, 2021). As the leading authority, the FIU collects all reports of unusual transactions. It examines these and disseminates the resulting intelligence to the relevant investigation and prosecution authorities.

Given the pivotal role played by the FIU in financial surveillance, it is remarkable how little is known about the daily operations of this relatively new organization. There is a growing literature that focuses on the increasing use of financial data for security purposes (Amicelle, 2017b), the role of banks and technology in combating terrorist

financing (Bosma, 2019), and lawsuits arising from these security efforts (Anwar, 2020). However, the exact role that the FIU plays in the wider financial surveillance system has remained largely unexamined, with few notable exceptions, such as research investigating how banks and FIUs collaborate (Amicelle, 2017a), how FIUs collaborate at the European level (Lagerwaard, 2020), and the legislative framework in which the FIUs carry out their activities (Mouzakiti, 2020). However, to my knowledge, there is as yet no detailed study of the daily practices of a particular FIU. In addition, the surveillance literature pays scant attention to this particular form of *financial* surveillance. The FIU is neither a conventional 'Orwellian' public security service, as it uses private payment data (Orwell, 1949), nor is it a large private company, like Google or Facebook, that uses its databases to monitor behavior for commercial purposes, labelled by Zuboff as "surveillance capitalism" (2019).

It is important to understand the operations of financial surveillance and the role of the FIU, because the intelligence that these organizations circulate includes sensitive private details, which raises questions regarding privacy and proportionality. FIU data contain not only details on specific financial transactions, but also a variety of other information that contextualizes the transactions, because a transaction in itself is not very informative. According to Ferrari (2020, p. 522), "Triangulated with other personal data points, [financial transactions] allow to infer information about individuals' activities, purchases and geographical movements, from which, in turn, sexual orientation, health status, religious and political beliefs and cultural preferences can be derived". Considerable public debate has focused on the collection of personal data by private companies, such as Google and Facebook (Van Dijck, 2014; Zuboff, 2019) and the use of artificial intelligence (Timan & Grommé, 2020). But dissemination of financial intelligence in which transactions form the basis of digital risk profiles that are compiled on citizens has not generally been associated with privacy and proportionality concerns (exceptions are Dehouck & De Goede, 2021; Mitsilegas & Vavoula, 2016; Riemslag Baas, 2021). Financial information is increasingly used by commercial companies (Westermeier, 2020), such as the so-called FinTechs, which are companies whose primary focus is on the development and implementation of financial technologies (Hendrikse et al., 2018). But the use of these data by *public* actors, such as FIUs, remains obscure. This difference is important because, as Mouzakiti (2020) argues, FIUs can be held to different legal frameworks, such as the General Data Protection Regulation (GDPR), investigative frameworks, such as the European Police Data Protection Directive, and in the Netherlands, the Dutch Police Data Act. Because data on millions of transactions are collected, analyzed, declared suspicious, and stored in databases *without* informing the persons or companies that carried out the transaction, a thorough understanding of financial surveillance and the role of FIUs is important, as they affect the privacy of anyone with a bank account.

This chapter examines the core tasks of FIU-the Netherlands and places these

tasks in the context of the wider financial surveillance system. It asks how the FIU, in practice, fulfils its three core tasks of *collecting*, *analyzing,* and *disseminating* (financial) information, and how it operates as a crucial pivot in the financial surveillance system. The study entails methodological challenges because certain activities were not accessible for research, due to the secrecy that is part and parcel of FIU operations. In particular, FIUs' actual analysis process is confidential. In the Netherlands the FIU database is classified as a state secret, meaning that no direct reporting on it may be published. This chapter 'encircles' that secrecy, by consulting sources that provide insight into the daily operations of FIU-the Netherlands (Bosma et al., 2019; see also Bellanova & Sætnan, 2019). The chapter concentrates on daily practices within the FIU, on organizational processes, and on dilemmas and challenges that were identified anonymously and without reporting potentially sensitive information. The 'encircling' method is supplemented by document analysis and semi-structured interviews with employees of FIU-the Netherlands and other European FIUs, allowing generic sources to be empirically situated.

The next two sections discuss, respectively, the theoretical background of financial surveillance and the method of 'encircling' secrecy. The bulk of the chapter then comprises three empirical sections, each dealing with a core task of the FIU: collecting, analyzing, and disseminating financial intelligence. The conclusion formulates several points of interest that can serve as an input for both further research and wider political debate on financial surveillance and the role of the FIU.

3.2 Financial surveillance

Surveillance is a broad concept that is often applied with various nuances. Perhaps the best-known and most imaginative concept of surveillance is the Orwellian Big Brother: a state dictator who leads a centralized power and has "thought police" which keep a close eye on the population's behavior via television screens (Orwell, 1949, p. 2). This classic interpretation of surveillance follows a Weberian approach, in which the focus lies on the state and bureaucracy (see, e.g., Dandeker, 2007, p. 40). Another imaginative concept of surveillance is the Foucauldian panopticon: the watchtower with tinted windows in the middle of a circular prison. From a position in the watchtower, the prison guard does not *have to* look but *possibly* looks, leading inmates to self-discipline (Foucault, 1977). Beyond these two key concepts, there are many other approaches to surveillance, such as the modern 'fluid' form of surveillance in which power and responsibilities are decentralized (Bauman & Lyon, 2013), and the surveillance of technology and large digital data sets that produce 'data doubles' of individuals (Haggerty & Ericson, 2000). Lyon, Haggerty, and Ball (2012, p. 1) claim that "interest in surveillance studies has mushroomed, generating considerable excitement about the potential for new ways to

understand human behaviour".

It is surprising that a field as extensive as *financial* surveillance, which is geographically widespread across more than 160 countries, each with its own national FIUs, does not occupy a substantial position in surveillance studies. Surveillance studies traditionally focus on topics such as CCTV cameras in the public domain (Armstrong & Norris, 1999) and the surveilling role of the information state (Weller, 2012). However, lesser-known topics are also increasingly studied from the surveillance point of view, such as the use of smartphones to monitor health (Lupton, 2012) and the use of aircraft passenger data for security purposes (Bellanova, 2014; Bellanova & Duez, 2012). Yet financial surveillance does not occupy a prominent position in this literature, with some notable exceptions. In the aftermath of the 9/11 attacks, Atia (2007) identified increasing financial surveillance of Islamic groups; in Europe, Vlcek (2007, 2009) observed that incidences of terrorist financing provided legitimacy to the implementation of financial surveillance; and Amicelle (2011, p. 162) has argued for development of a new concept of financial surveillance – a new "political anatomy" – that includes multiple actors with heterogeneous aims (see also Amicelle & Favarel-Garrigues, 2012).

Related literature focusing not on surveillance but on the 'finance-security nexus' provides more information about the variety of actors involved in financial surveillance (Boy et al., 2017; De Goede, 2010; Langley, 2017; Westermeier, 2019). This literature explores the different ways in which finance and security are intertwined, such as the use of financial resources in war situations (Gilbert, 2015). This literature is increasingly interested in the use of financial transactions for security purposes (Amoore & De Goede, 2008; Boy et al., 2017). De Goede (2018) speaks of a "chain of financial security", in which financial transaction information travels from actor to actor, starting with commercial entities, such as banks, which monitor payment behavior; to the FIU, which carries out further analysis and forwards suspicious information to executive authorities. Eventually, the information may reach the courts, where it is used to convict a suspect. The transaction information does not remain the same as it travels through the chain; rather, it is "translated" and acquires a different meaning in each professional domain (De Goede, 2018, p. 29). According to De Goede, the FIU occupies a central position in this chain, between the commercial and public actors. However, "very little… is known about how FIUs handle, share, and analyse unusual transaction reports" (De Goede, 2018, p. 35; see also De Goede, 2017b).

This dissertation understands financial surveillance to be a broad-based collaboration between private and public actors who systematically monitor, filter, analyze, and use transaction information in order to ascertain the spending behavior of citizens, with the objective of detecting and, if possible, prosecuting and punishing criminal misconduct. The FIU is perhaps the most important actor, the pivot, in this system, because it is the only actor that operates purely at the intersection of finance and security. As a metaphor, this pivotal role can be likened to an hourglass. In the Netherlands, information on unusual

financial transactions flows like sand from 25 professional groups – not just financial entities – that are required by law to report unusual transactions to the FIU (FIU-Nederland, n.d.). The FIU forms the center of the hourglass. However, the FIU does not let all the sand pass. Instead, it monitors, selects, modifies, and filters what it receives, after which it sends the intelligence it deems suspicious to a broad spectrum of police, justice, and security services in the security chain.

What makes the FIU so interesting is that it operates as a pivot at several intersections. First, the FIU operates at the intersection of *finance*, entailing the world of banking and economic transactions, and *security,* which is the world of the police, secret services and judicial authorities. It also acts as a pivot at the intersection of *private* actors, as it depends on private transaction data, and *public* authorities, to whom it must forward the intelligence for security purposes. The FIU itself is an intersection, where *unusual transaction information* goes in and *suspicious financial intelligence* comes out. Finally, the FIU operates at the intersection of the national and international domains, as it plays an important role in sharing intelligence with FIUs in other countries in order to identify and trace international money flows (Amicelle & Chaudieu, 2018). It is surprising that, given this pivotal position, the FIU's specific role in the wider financial surveillance system remains obscure, both in the academic literature and in political and policy-related debate.

3.3 The 'encircling' of secrecy

To investigate the secret processes at the FIU, I made use of the method of "encircling" secrecy (Bosma et al., 2019, p. 14). The FIU's data, such as the actual unusual transactions, are categorized as a 'state-secret secret' at the time they are entered into the FIU database. This is one of four categories of sensitive information within the Dutch government; these being 'departmental confidential', 'state-secret confidential', 'state-secret secret', and 'state-secret very secret' (VIRBI, 2013). The FIU data fall into the third category – state-secret secret – meaning that specific security measures apply, such as registration of all persons to whom the information is disclosed, the signing of a nondisclosure agreement, and the possession of a so-called 'certificate of no objection' (*verklaring van geen bezwaar, VGB*) (ibid.). This secrecy is not without reason. The information that the FIU works with is privacy sensitive. Any revelation of precise investigations by the FIU to individuals whose information is retained could be harmful to the investigation and eventual prosecution, as well as to the individuals or companies concerned. The nondisclosure agreement, in particular, makes it difficult for researchers to examine authorities such as the FIU, because without consent there is no possibility to examine the analysis process, but with consent restricted publication of results is allowed.

There is a growing literature on secrecy (Birchall, 2016) and the methodological issues that it raises (Belcher & Martin, 2019; De Goede et al., 2019; Dijstelbloem & Pelizza, 2019). Bosma, De Goede, and Pallister-Wilkins (2019, p. 3) address this difficulty: "We do not consider closed doors, partial visibilities and obfuscation necessarily to constitute failed research. Instead of considering what has been lost or what stays out of the picture, we ask, what does mapping the contours of secrecy and obfuscation *add* to our analysis?" Secrets have the stature of authenticity because they are difficult to verify (Jones, 2014). This does not mean, however, that secrets 'must be revealed', because it is possible to research the status and meaning of a secret without knowing the actual contents. In the case of the FIU, the content of the secret is not incomprehensible, but the data analysis process is in fact routine – and even a little boring. The secret is not an irresolvable hurdle that prevents detailed study. The research approach taken here is therefore not oriented at revealing confidential information or practices, but at 'encircling' the obstacle that secrecy poses in a creative methodological manner, and thus obtaining a thorough understanding of financial surveillance and the FIU. According to Bosma, De Goede, and Pallister-Wilkins (2019, p. 14), encircling implies "a lateral, multipronged, creative, iterative approach to secret sites, confidential materials, and classified practices. It is less focused on uncovering the *kernel* of the secret, than it is on analysing the mundane lifeworlds of security practices and practitioners".

As part of my research on the analyses processes of the FIU, I completed in 2017 the operational analysis e-learning course offered by the International Centre for Asset Recovery of the Basel Institute on Governance.[12] This course is intended for FIU analysts and covers, among other things, the core tasks of an FIU analyst, analysis of suspicious transaction reports (STRs), collection of information from open and closed sources, and dissemination of findings. The course, which was particularly valuable in informing the empirical part of the research, was *not* specifically about the analysis practices of FIU-the Netherlands. To understand specifically the practices of FIU-the Netherlands, I obtained up-to-date details from the annual reports of FIU-the Netherlands, which were publicly accessible.[13] In addition, this chapter's analysis is based on five semi-structured interviews with employees at FIU-the Netherlands and eight interviews with employees at FIUs elsewhere in Europe. To safeguard the anonymity of respondents, no direct quotes or references are used in this chapter. Triangulation between these three sources made it possible, in an ethical manner, to 'encircle the secrecy', to examine the core tasks of the FIU, and to address important issues, such as privacy, proportionality, and accountability, which – hopefully – will inform a broader political and academic debate.

12 See https://baselgovernance.org/elearning-courses/operational-analysis-english, consulted on April 28, 2021.

13 For annual reports, see https://www.fiu-nederland.nl/nl/over-fiu/jaaroverzichten, consulted on June 14, 2021. This chapter often refers to the 2020 report for data on 2019; and the 2021 report for the data on 2020; because these provided the most up-to-date information at the time of this writing.

The next three sections discuss the core tasks of the FIU. In practice, these overlap somewhat because as the transaction information travels through the chain it is gradually modified and 'translated' in understanding (De Goede, 2018; see also Latour, 1999). These empirical sections discuss the *collection* of unusual transactions by commercial actors, the *analysis* of this data through scrutiny and research, and the *dissemination* of suspicious intelligence to domestic and foreign investigation and prosecution authorities. Each section concludes by raising a number of issues, which will be further addressed in the conclusion.

3.4 Collection of transaction information

The collection of transaction information is the foundation on which the FIU, as well as the wider financial surveillance system, functions. Without this information, the FIU cannot provide any contribution to the investigation and prosecution services. Since the inception in 1994 of the Office for the Disclosure of Unusual Translations (abbreviated as *MOT*, the Dutch acronym for *Meldpunt Ongebruikelijke Transacties*), the number of reported transactions has increased substantially: from 16,215 unusual transactions in 1995, of which 2,218 were deemed to be suspicious, to 722,247 in 2020, of which 103,947 were declared suspicious. Every 24 hours, the FIU receives about 1,200 to 1,400 reports, which are stored in a transactions database containing an average of 1.2 to 1.4 million unusual transactions (Akse, 2019, pp. 5–8). Who sends this transaction information to the FIU? On what grounds are the selected transactions reported? How are they submitted and stored?

The FIU receives transaction information from various reporting groups, which the media often refer to as 'gatekeepers' of the financial system. These reporting groups consist not only of banks, but also many other professional groups with access to certain transaction data and payment services. It is mandatory for them, too, to report unusual spending behavior and transaction patterns to the FIU, pursuant to the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme, Wwft*). They are deemed to be responsible for detecting – not only financial – crimes, such as corruption, drug-related activities, trafficking in human beings and smuggling, fraud, healthcare fraud, misuse of virtual assets, money laundering, terrorist financing, and other forms of crime (FIU-Nederland, 2020, p. 10). There are 25 professional reporting groups, including accountants, lawyers, investment firms, cryptocurrency traders, intermediaries, payment service providers, tax consultants, legal service providers, casinos, brokers, and sellers of luxury goods, such as gold dealers, car dealers, boat sellers, and, since recently, art dealers (ibid., p. 50; also FIU-Nederland, n.d.). It can be said that financial surveillance and combating financial crime have been woven into the very fabric of the economy.

The millions of unusual transactions that reporting groups submit contain not only financial information, but also supplementary details to place the transaction in a broader context. The initial unusual transaction report from the reporting entity must include the following information based on the *Wwft*:

a. the identity of the client, the identity of the ultimate beneficial owners…
b. the nature and number of the client's identity document…
c. the nature, time and place of the transaction;
d. the amount as well as the destination and origin of the funds…
e. the circumstances under which the transaction is deemed to be unusual;
f. a description of the particular valuable items in a transaction above €10,000;
g. additional details, designated by order in council (Ministry of Justice, Netherlands, 2008, sec. 16, 2).

In other words, when reporting an unusual transaction, the actual financial transaction forms only the basis for a broader account and (digital) profile of the individual or company that undertook the transaction. Points (a) through (d) cover the general 'absolute' data, such as the client's identity document,[14] the nature and time of the transaction, and the amount. Point (g) means that the FIU can submit an inquiry to the reporting entity for additional information. Points (e) and (f) require further explanation, because these highlight two features of financial surveillance that are essential to understand the entire process of collection, analysis, and dissemination. Reporting groups, including those in other countries, must report a transaction based on *objective* or *subjective* indicators. Point (f) is an example of an objective indicator. Any transaction with a value greater than €10,000 must be investigated. In the case of banks, for example, transactions such as cash deposits of this size *must* be reported (FIU-Nederland, n.d.a). When the 'threshold' is adjusted upwards or downwards, it automatically causes an increase or decrease in the number of reports of unusual transactions to the FIU. Another objective indicator is the assessment of risk countries, as designated by the European Commission (2016) and the Financial Action Task Force (FATF).[15] *All* transactions with these countries must be marked as unusual and reported to the FIU. The objectivity of objective indicators, therefore, relates not to the indicators themselves – as these are based on certain assumptions – but derives from the fact that they can be implemented 'objectively', often by automated monitoring systems.

The subjective indicators, in contrast, require reporting entities to consider the risk of a transaction, based on personal, normative assumptions about a customer's payment

14 Reporting groups such as banks are expected to implement a 'know your customer' policy. In doing so, they are expected to identify, verify, and in the case of entities such as companies or foundations, to establish the 'ultimate beneficial owners'.
15 See for high risk countries https://www.fatf-gafi.org/countries/#high-risk, consulted on June 8, 2021.

behavior. Point (e) is an example, as it requires the reporting entity to describe the circumstances that classify the transaction as unusual. The Tax and Customs Administration of the Netherlands interprets this point as the answer to the following question: "Why do you find the transaction to be unusual?" (Belastingdienst, n.d.). While the FIU prescribes five objective indicators for banks, for the subjective indicator only the following description is given: "A transaction for which the institution has reason to believe that it may be related to money laundering or terrorist financing" (FIU-Nederland, n.d.a). This subjective indicator is open to interpretation and relies on the commercial reporting person's ability to recognize a crime or financial criminality. In certain sectors, regulators do provide guidelines for implementing the subjective indicator, such as the Dutch Authority for the Financial Markets (AFM, 2020) and De Nederlandse Bank (DNB, 2020), but these are not policy rules and are not legally binding. It is therefore the normative suppositions of commercial operators that, to a considerable extent, form the 'front line' of financial surveillance – that is, providing the information on which the chain of financial security and the combating of financial crime is vested (De Goede, 2017a).

The number of reported unusual transactions rose significantly from 2010 to 2020 (Figure 3.1). Reporting groups submit their reports via a reporting form or XML report.[16] The reporting form is often used by minor reporting entities, such as sellers of luxury goods that do not report very often (FIU-Nederland, n.d.). XML reports are used by major reporting entities, such as banks, which have automated reporting systems with their XML – a structured format harmonized to the FIU's XML. The capacity of reporting groups to invest and the number of reports they submit varies considerably. For example, in 2020, casinos reported 3,764 unusual transactions, while banks reported 245,148 unusual transactions. An important observation about Figure 3.1 and these statistics, is the fact that the substantial growth registered in 2019 was mainly the result of a reinterpretation of the 'risk countries'. This objective indicator was responsible for as many as 1,921,737 unusual transaction reports in 2019 (FIU-Nederland, 2020, p. 31). In order to reduce this flood of reports, this objective indicator was changed to a subjective indicator in 2020, meaning that reporting entities were again required to assess and decide for themselves what a risk country exactly is (ibid.). The rise in numbers of reports, therefore, cannot be understood as reflecting an actual increase in unusual financial behavior in society. The 2019 increase illustrates that it is the frameworks of and compliance with the indicators that largely determines increases or decreases in number of unusual transaction reports.

In view of the substantial number of unusual transactions received by the FIU from the 25 reporting groups in the Netherlands – as the complement of employees involved in such reporting at banks alone numbers more than 12,000 (Kamphuis, 2021) – the FIU

16 See for the online reporting portal: https://meldportaal.fiu-nederland.nl/Home, consulted on June 8, 2021.

might be expected to have a large staff as well. However, the FIU is a relatively small organization, with a workforce of 76 employees in 2020 (FIU-Nederland, 2021, p. 16). Its financial capacity is also limited compared to banks. The major banks in the Netherlands have invested billions in monitoring unusual financial transactions. The ABN Amro bank alone invested more than one billion euros by 2021 and is planning on investing another billion (De Boer, 2021). The FIU, on the other hand, had an annual budget of €9 million in 2021 (FIU-Nederland, 2021, p. 16). These ratios raise the question of proportionality: Is the input from the reporting groups in proportion to the effectiveness of the FIU? Moreover, it suggests a practical dilemma: given the millions of unusual transactions reported and the limited human and financial capacity of the FIU, the FIU's task would seem overwhelming. How does FIU-the Netherlands analyze the unusual transactions reported to it, as these number more than a thousand every day?

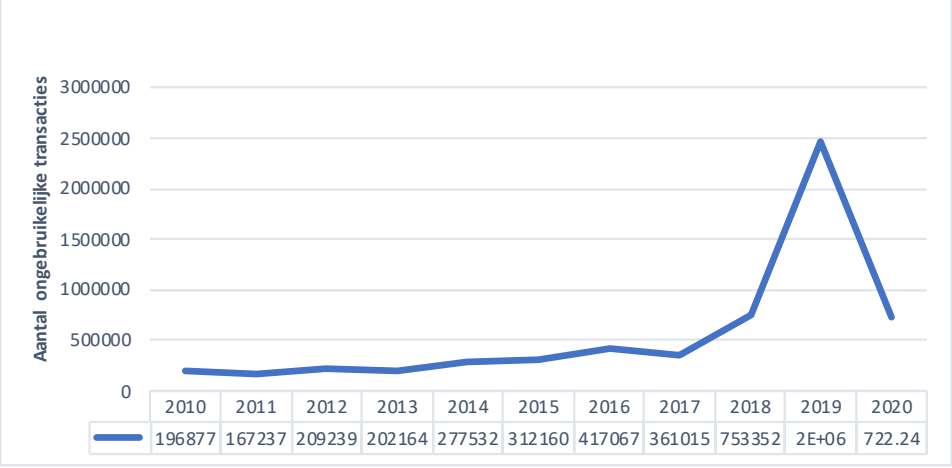


FIGURE 3.1: Longitudinal overview of the number of unusual transactions at FIU-the Netherlands. Source: Author, based on previous fieldwork (Lagerwaard, 2018) and information from the annual reports of the FIU (FIU-Nederland, 2019, 2020, 2021).

3.5 Analyzing the data

> FIU-the Netherlands' unusual transactions database is full of transactions that could imply money laundering or other forms of criminality. With the current capacity at FIU-the Netherlands and also the capacity of investigative authorities, it is neither possible nor desirable for that matter to conduct equally thorough investigations of all transactions. FIU-the Netherlands has developed a strategic control and tactical selection model, which, as far as possible, enables the correct issues to be investigated, which is also in line with the priorities of the acquiring investigation partners (FIU-the Netherlands, 2020, p. 59).

This section discusses the process from the moment an unusual transaction is reported until the financial intelligence leaves the FIU. This process is not linear, with a transaction being reported, then examined, then declared suspicious or not, and then forwarded or not. Rather, it is *source-based*, in which the entire database of unusual transactions, also known as the "buffer", mediates between reporting and investigation (Akse, 2019, p. 38; FIU-Nederland, 2020, p. 55). The unusual transactions database – having 1.2 to 1.4 million reports – is updated every day, and new reports are stored for five years (FIU-Nederland, n.d.e). The database is therefore not so much a static storage place, where information is deposited and digitally retained until it is destroyed, but an active investigative resource that is continuously changing. Given the capacity ratio between the reporting groups and the FIU, this source-based strategy is essential because it makes it possible to select which reported unusual transactions will be subjected to follow-up investigation. This is done by routinely performing searches of the *entire* database based on new external research data and queries. On what grounds is an unusual transaction declared suspicious? What type of analysis does the FIU itself perform? How is transaction information transformed into financial intelligence? This section first looks at the process by which an unusual transaction is declared suspicious, after which it investigates the analysis methods of the FIU, drawing on the *operational analysis* course.

Declared as suspicious

A typical feature of the Dutch financial surveillance system is the distinction between *unusual* and *suspicious* transactions. Reported transactions are in first instance 'unusual' and can be declared suspicious only by the FIU. The methods by which suspicious transactions are filtered from the unusual transactions database can be roughly divided into two groups: semi-automated methods – often referred to as *analysis* – and the manual methods – often referred to as *investigation*.

The semi-automated methods link the database of unusual transactions to external information sources, such as sanctions lists, databases, and other data files. The most important national database that is interfaced is the Index of Criminal Investigations and Subjects – Dutch acronym *VROS* (*Verwijzingsindex Recherche Onderzoeken en Subjecten*) – which is a national police force database containing "criminal intelligence unit subjects and subjects under investigation by detectives" (KLPD, 2008, p. 174; see also FIU-Nederland, 2019, p. 23).[17] In 2020, 42,367 transactions were declared suspicious because of matches between the FIU database and the Index of Criminal Investigations and Subjects/*VROS*, representing more than one-third of the total number of suspicious transactions in that year (FIU-Nederland, 2021, p. 10). In addition, the FIU database is regularly compared to national database files at the Prosecution Service Criminal Assets Deprivation Bureau (in Dutch, *Bureau Ontnemingen Openbaar Ministerie, BOOM*) (KLPD, 2008, p. 174), the Central Fine Collection Agency (CJIB) (FIU-Nederland, 2020, p. 38), and the National Sanctions List of Terrorism (ibid., p. 42). Foreign national sanctions lists and international lists, such as those of the European Commission, are also compared (ibid.), and the database is made available indirectly and anonymously to FIU.net, the system with which the European FIUs exchange data.[18] Comparisons with this host of lists, databases, and links to other data files are considered semi-automatic, as the information sources automatically track down suspicious transactions from *within* the database, without having to perform specific queries.

Manual methods, on the other hand, require *external* input for targeted searches in the database. Requests for these come primarily from the National Public Prosecutor (*LOvJ*), which is charged with this task as an intermediary for the investigation and prosecution authorities. Based on these requests for information, the FIU consults the database, declares matching unusual transaction information as suspicious, and after possibly conducting further investigation, provides the intelligence (Audit Magazine, 2019, p. 21). In 2020, the FIU received 1,213 National Public Prosecutor requests from 23 different organizations (Figure 3.2). Another important manual method is the exchange of information with foreign FIUs. The National Public Prosecutor may request FIU-the Netherlands to apply for information from a foreign FIU, and foreign FIUs may submit requests to FIU-the Netherlands (FIU-Nederland, 2020, p. 32). In 2020, FIU-the Netherlands received 650 requests for information from 77 foreign FIUs, and FIU-the Netherlands itself submitted 590 requests to 85 foreign FIUs (FIU-Nederland, 2021, p. 7). Such exchanges can take place through what is known as *diagonal cooperation*, in which the FIUs act as a mailbox that forwards information to a national investigation

17 Citing from a parliamentary paper, "This VROS index not only includes investigations relating to criminal intelligence unit subjects, but also all investigations that last longer than a week and are aimed at crimes for which provisional custody is permitted" (Dutch House of Representatives [Tweede Kamer], 1998).

18 This database of unusual transactions is anonymously compared in FIU.net. The foreign FIU can use this information only after further consultation and a transaction officially being declared as suspicious.

or prosecution service (Amicelle & Chaudieu, 2018, p. 652; European Commission, 2017, p. 4). As requests from the Netherlands' National Public Prosecutor have become increasingly complex, the FIU planned to semi-automate these inquiries in the future as well (FIU-Nederland, 2020, pp. 6 & 9).

National police		Other investigative services	
Zeeland West-Brabant Police Unit	107	Fiscal Intelligence and Investigation Service (FIOD)	210
Central Netherlands Police Unit	106	Royal Netherlands Marechaussee (KMar)	189
Rotterdam Police Unit	78	Social Affairs and Employment Inspectorate (ISZW)	20
Central Unit of the National Police	75	District court public prosecutor's office	15
Amsterdam Police Unit	68	KMar Schiphol district	3
Eastern Netherlands Police Unit	60	National Office for Serious Fraud, Environmental Crime and Asset Confiscation	18
East Brabant Police Unit	56	National Police Internal Investigations Department	12
The Hague Police Unit	52	Social Security Fraud Department	13
Northern Nederlands Police Unit	37	Netherlands Food and Consumer Product Safety Authority - Intelligence and Investigative Service (NVWA-IOD)	13
Limburg Police Unit	38	Human Environment and Transport Inspectorate - Intelligence and Investigative Service (ILT-IOD)	6
North Holland Police Unit	34	National Public Prosecutor's Office	2
		Criminal Investigation Cooperation Team	1
Subtotal National Police	**711**	**Subtotal other services**	**502**

FIGURE 3.2: National Public Prosecutor requests per investigation or prosecution authority in 2020. Source: FIU-the Netherlands (2021, p. 35).

In sum, suspicious transactions derive from the active monitoring, filtering, and searching of the entire unusual transactions database. As a result, intensified use of semi-automated or manual methods can lead to an increase in suspicious transactions, which may be disproportionate to any growth or decline in the number of *unusual* transactions. For instance, even though the number of unusual transactions declined in 2020, the number of suspicious transactions that year increased considerably (Figure 3.3). Ultimately, the selected unusual transactions are officially declared suspicious by the Head of the FIU (FIU-Nederland, 2020, p. 54), after which the reporting entity receives an automatic 'confirmation of receipt' indicating that the unusual transaction

has indeed been declared suspicious (FIU-Nederland, n.d.e). The individual or company that undertook the transaction is not notified.

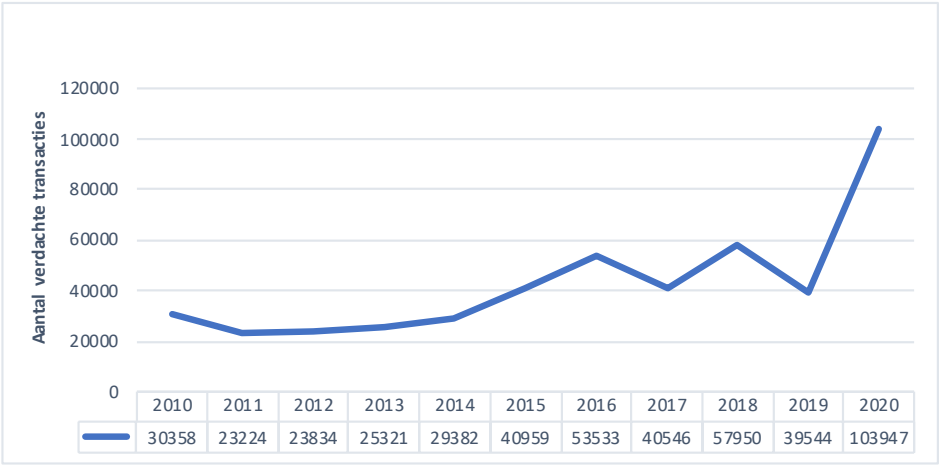


FIGURE 3.3: Longitudinal overview of the number of suspicious transactions at FIU-the Netherlands. Source: Author, based on previous fieldwork (Lagerwaard, 2018), and information from the annual reports of the FIU (FIU-Nederland, 2019, 2020, 2021).

The analysis process

FIU-the Netherlands makes the suspicious transactions widely available to investigative services – which will be dealt with in the next section – but it also performs its own supplementary analysis. Suspicious transactions that are mutually associated are merged into 'files' – for example, the 103,947 transactions declared suspicious in 2020 were merged into 19,114 files (FIU-Nederland, 2021, p. 7), with about five transactions per file. In practice, the size of a file depends on the topic, investigative capacity, and the importance of the intelligence to the investigating agents further down the chain. A file may therefore contain one or even thousands of transactions (FIU-Nederland, 2021, p. 10). Due to the FIU's own limited investigative capacity, each year it selects a number of topical themes, such as trafficking in human beings, drug trafficking, and "gaining insight into healthcare fraud" (FIU-Nederland, 2020, pp. 33–35). Policy priorities are defined by an FIU administrative body, known as the strategic steering committee, and a body to which proposals for investigations can be submitted, the tactical selection committee, which assesses proposals and determines the required capacity (ibid., p. 60).

According to the operational analysis course, an FIU analysis consists of an 'intelligence cycle', entailing seven steps: planning, collecting, evaluating, collating, analyzing, reporting, and disseminating. The first step, planning, concerns the selection

of suspicious transactions that are to be investigated further. In the case of FIU-the Netherlands, this is largely determined by the tactical selection committee. The second step, collecting, focuses on the gathering of supplemental information. The course emphasized that this will depend on the investigative capabilities of an FIU in legal terms, and the resources the FIU has access to. The collection of resources follows several steps, which can be visualized as a pyramid, as shown in Figure 3.4. At the top of the pyramid are the STRs, which is the information that a reporting entity has submitted. The FIU then consults its own information, drawing on previous investigative experience and knowledge. In the case of FIU-Netherlands, for example, the themes selected by the strategic steering committee result in an accumulation of knowledge on certain topics. This can be consulted during investigations.

At the bottom of the pyramid are national and international open and closed sources. FIU-the Netherlands consults several *closed* national sources, such as Infobox Criminals and Inexplicable Assets (FIU-Nederland, 2020, p. 33), tax data (which can be requested) (ibid., p. 59), and police systems to which the FIU is connected. Closed international sources, according to the course, are derived from cooperation with foreign organizations, such as Europol, Interpol, and foreign FIUs. In particular, FIUs have committed to freely share as much intelligence as possible, including their own closed sources with their FIU counterparts (Egmont Group, 2013, 2017). *Open* sources may include publicly available information, such as the commercial register of the Chamber of Commerce, but also the variety of information accessible via the internet: Google search results, annual reports of organizations, company websites, journalistic articles and programs, scientific research, and social media, such as Facebook, Twitter, and Instagram. FIU-the Netherlands makes use of open source intelligence, for which it developed special software in 2019: "[to make] open sources more easily available and to train researchers in this" (FIU-Nederland, 2020, p. 14). The third step of the intelligence cycle, evaluating, comprises an assessment of the reliability and validity of the found information. Step four, collation, is the arranging of the information in preparation for the analysis.

Step five, analysis, comprises several elements: a thorough study of the sources, formulation of a hypothesis, conducting further research, and ultimately formulation of a substantiated argument. According to the course, this step is supported by numerous analytical methods, such as the use of an association matrix, in which sources are connected and correlations determined, or a link chart, in which information and correlations can be visualized. FIU-the Netherlands works with different methods of analysis. It states, for example, that "by using a high-performance reporting and analysis tool", it produces targeted reports and analyses, with which it "tries to identify so-called red flags through qualitative research, which can filter precisely those transactions from the database that are linked to a certain type of crime" (FIU-Nederland, 2020, p. 59). From the case studies released by FIU-the Netherlands, it can be concluded that different

analysis methods are used. For example, the FIU applied "network analysis" for an investigation of cross-border flows of funding (ibid., p. 17); it carried out "transaction analyses" on drug and letting offences (ibid., p. 18) and criminal organizations (Akse, 2019, p. 73); and it produced "financial profiles" to investigate trafficking in human beings (ibid., p. 60), illegal exchange practices (FIU-Nederland, 2020, p. 27), and terrorist financing (ibid., p. 43).

According to the course, during the analysis process a transformation takes place from simple financial *information* to financial *intelligence*. Information "is raw data. It is knowledge communicated or received concerning some fact or circumstance" (Basel Institute on Governance, 2017). Intelligence, on the other hand, consists of inferences from this information, supplemented by analysis and arguments that give meaning to the information. In the course, intelligence was defined as a "value-added product derived from the collection and processing of all relevant information relating to the end user's needs.… [Intelligence] is immediately or potentially significant to the end user's decision-making process" (ibid.). FIU-the Netherlands is not merely an intermediary of information from private parties to public authorities. It also influences and mediates certain information by analyzing, filtering, and investigating transactions, providing more information on transactions. Based on this process, it forms arguments and merges its results into files which it forwards as intelligence. Steps six and seven of the intelligence cycle, respectively, focus on the reporting and disseminating of financial intelligence, the subject of the next section.

In sum, the source-based approach offers a solution to the unbalanced ratio between the millions of unusual transactions reported by the plethora of reporting groups, and the FIU, which has only limited financial and human capacity to examine these. The time limit of five years of storage in the database is important, because the source-based approach does not work when data are stored for just a month, or if data were immediately destroyed once deemed inapplicable. However, the source-based approach raises a number of issues concerning privacy and proportionality. Because unusual transactions are selected by commercial actors without intervention, for instance, by a public prosecutor or investigating judge, it actually constitutes a large-scale database of information on citizens who are not officially suspects of wrongdoing – a database of 'non-suspects'. Individuals and companies from which the – not only financial – information has been derived, are not informed that their data are in the database. Moreover, the *Wwft* and the FIU have no processes whereby individuals or entities may opt to be informed of whether their personal data appear in this database. By retaining information on millions of private transactions of non-suspects for a period of five years, the question of proportionality becomes key: Is such systematic collection and storage of private data on non-suspects in proportion to the security revenues? This question becomes increasingly pressing when considering that the unusual transaction information may be copied and stored in the database dedicated to *suspicious* transactions

– which is actively disseminated among investigation and prosecution authorities and with foreign FIUs around the globe.

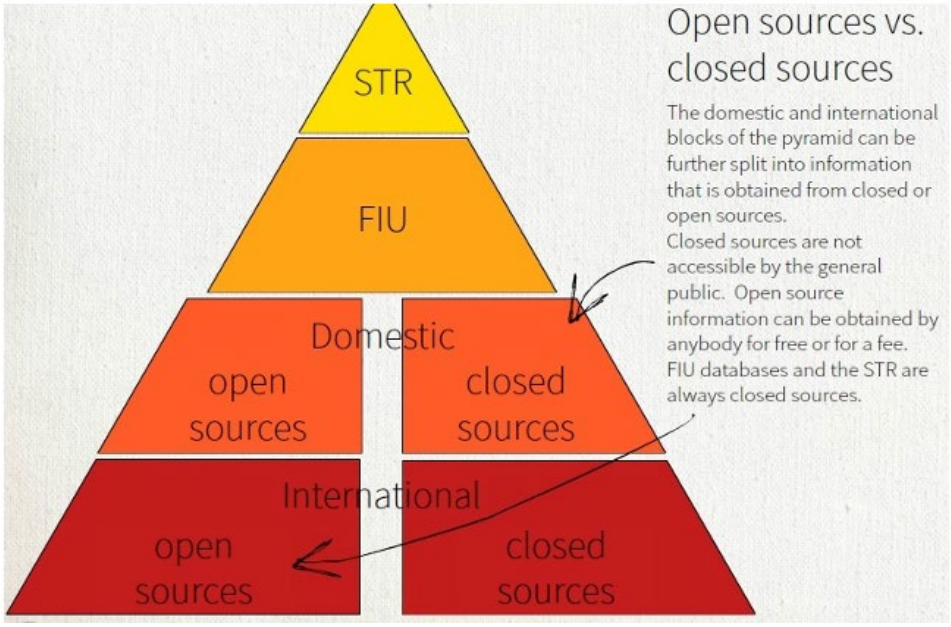


FIGURE 3.4: Collection of open and closed sources. Source: Basel Institute on Governance (2017).

3.6 Dissemination of intelligence

> Investigative services that acquire the most FIU information are the National Police and the FIOD [Fiscal Intelligence and Investigation Service]. FIU-the Netherlands commits to both widespread and targeted dissemination of FIU intelligence through an application to which virtually the entire police force has access. FIU-the Netherlands targets dissemination by making arrangements with those customers that acquire the information (FIU-Nederland, 2020, p. 59).

This section examines how FIU-the Netherlands 'markets' its financial intelligence. The FIU cannot take action on its own accord because it is not authorized to apprehend or prosecute suspects. Yet, the FIU is the pivot in financial surveillance. Operating at various intersections, it must bridge gaps, such as that between those reporting and those

investigating, though without policing powers of its own. The pivotal position is possible because of its exceptional institutional embedding. On the one hand, reporting groups submit their unusual transactions without dealing directly with the police. On the other hand, the FIU is operationally embedded in police procedures. FIU-the Netherlands is a so-called "hybrid FIU", meaning that it is delegated to the police but falls under the responsibility of the Minister for Justice (Akse, 2019, p. 38). The *Wwft* demarcates this hybrid position.[19] The Minister for Justice is responsible for the organization's general management. The Minister of Finance is responsible for its budget; and the Head of the FIU – the director – is appointed by agreement between both ministers. In practice, the hybridity becomes even more versatile at an organizational level, as the FIU is an independent organization embedded in the police (Akse, 2019, p. 44; FIU-the Netherlands, 2020, p. 54). This means that it must adhere to, for example, the Police Data Act (*Wet politiegegevens, Wpol*). Although the FIU is not a police authority *pur sang*, it does have access to the police's systems and networks and is able to disseminate its intelligence via these infrastructures (Akse, 2019, pp. 35 & 38). How and to what actors does the FIU make the suspicious transactions database available? How does the FIU actively contribute to investigations and follow-up initiatives? How is the intelligence ultimately used?

There are two different types of dissemination: making the database of *suspicious* transactions available to third parties and actively collaborating with those public authorities that are interested in financial intelligence. Similar to the unusual transactions database, analysis of the suspicious transactions database is not done in a linear fashion, in which the intelligence is sent and investigated further, resulting in a final ruling. Rather, it too is *source-based*. All unusual transactions that are declared suspicious by the Head of the FIU are copied into a separate database of only suspicious transactions. That database contained 438,240 transactions in 2020. Transactions belonging to files which were eventually deemed not suspicious after further investigation by the FIU – 1,645 of the 5,302 files in 2019, with an unknown number of transactions – are also retained in this database (FIU-Nederland, 2020, p. 38). The transactions in the suspicious transactions database are stored not for five years but for ten years, so the database covers a broader timeframe than the database of unusual transactions. In addition, these suspicious transactions are more informative than unusual ones, because they are connected to files and may be supplemented with additional intelligence from open and closed sources.

Unlike the database of unusual transactions, which is in the FIU's protected possession and accessible only to FIU employees, the database of suspicious transactions is made available externally (Akse, 2019, p. 38). The data can be accessed via BlueView,

19 In particular, sections 12, 13, and 14, respectively, set out the institutional embedding, core tasks and responsibilities, and juridical framework of the FIU.

a police system that was comprehensively introduced in the Netherlands in 2007 and is available to all investigative authorities (FIU-Nederland, n.d.e). BlueView includes "all records in the Netherlands of official reports submitted to the police, of hearings, official reports, files, reports and documents relating to confiscated goods…, as long as they are not older than five years" (AG connect, 2008). The BlueView system has been typified in news media as a way to 'Google' criminals (see Nu.nl, 2007). By making the database of suspicious transactions available through BlueView, 'old' data can appear useful many years later, based on new investigation and intelligence gathering. The database of suspicious transactions is accessible on a national scale to investigative services in the Netherlands, such as the police; special intelligence agencies; intelligence services; security services; the Public Prosecution Service; the National Office for Serious Fraud, Environmental Crime and Asset Confiscation; and the Netherlands' 10 Regional Information and Expertise Centres (RIECs).[20]

The second way in which FIU-Netherlands disseminates financial intelligence is through actively collaborating with public organizations, both *bilaterally* and *multilaterally*. At a bilateral level, there is direct collaboration on some files, particularly those which the FIU has designated the status of 'suspicious embargo'. In 2020, there were 65 files of this kind, involving a total of 1,725 transactions (FIU-Nederland, 2021, p. 34). These were "included in detective work, intelligence gathering, and security investigations which, in connection with strict confidentiality, were only shared with the service or services involved in the investigation" (FIU-Nederland, 2020, p. 38). In addition, the FIU has several 'main customers' such as the National Police and FIOD. They not only make use of the database and National Public Prosecutor requests, but also have targeted ways of collaborating in which the FIU shares 'broader views' and 'specialist knowledge', including with regional police units (ibid., p. 18). The FIU might also collaborate with a partner on a particular type of crime. For example, in the case of terrorist financing, it might collaborate with the General Intelligence and Security Service (AIVD) and Military Intelligence and Security Service (MIVD). In regard to trafficking in human beings and healthcare fraud, it might partner with the Social Affairs and Employment Inspectorate (ISCW) (ibid., p. 20), with which it produced a "healthcare fraud monitor" in 2020 (ibid., p. 35).

FIU-the Netherlands also participates in several public-private, or public-public partnerships (PPPs), in which a variety of public and/or private parties are involved in combating a particular issue. For example, the FIU is part of the Financial Expertise Centre (FEC), a collaboration that aims to strengthen the integrity of the financial sector and comprises the police, FIOD, FIU, and Public Prosecution Service, as well as the Tax and Customs Administration, the regulators of the Dutch central bank (DNB), and

20 The RIECs use these suspicious transactions, for example, to organize 'confiscations' from criminals (RIEC-LIEC, 2020, p. 22).

the Dutch Authority for the Financial Markets (AFM). Furthermore, at the national level, the FIU is part of the Serious Crime Taskforce (SCTF), the Fintell Alliance (FIU-Nederland, 2020, p. 19), the Terrorist Financing Taskforce (TF-Taskforce) (DNB, 2019), the Financial Intelligence Centre (FIC Rotterdam) (FIU-Nederland, 2020, p. 20), and the interdepartmental working group Freezing Consultation (ibid., p. 42). At the international level, it is part of the Europol Financial Intelligence Public Private Partnership (EFIPPP), the Egmont Group of FIUs, and the EU FIUs Platform. The FIU contributes to these collaborations not only with its own expertise and database of suspicious transactions – to which certain other actors also have access – but also via its role as the sole entity with access to the database of *unusual* transactions. In these collaborations, banks can pass on unusual transactions that the FIU can declare suspicious, therefore rendering them accessible to the investigation and prosecution services via the suspicious transactions database (ibid., p. 45). In this way, the three core tasks of the FIU combine in practice.

Despite these different forms of intelligence dissemination, it is difficult to procure an estimate of the scope to which financial intelligence is actually deployed by the investigative and prosecution services. To my knowledge, there is no quantitative data available on how financial intelligence is eventually used for investigation and prosecution. In the annual reports of the FIU and on its website, the FIU offers casuistry for its activities related to COVID-19 benefit fraud, a "rogue letting agency", the financing of terrorism, money laundering, tax evasion, and healthcare fraud, in which the intelligence of the FIU was important (FIU-Nederland, n.d.c). However, this reportage is anecdotal, and both for money laundering and terrorist financing – the FIU's two core tasks according to the *Wwft* – it is estimated that the number of resultant lawsuits is no more than a couple of dozen. Between 2015 and 2020, there were about 20 terrorist financing cases.[21] Yet, it is unclear how many of these originated from the FIU's suspicious transactions. Furthermore, no details are known regarding numbers of money laundering cases. In the media, an employee at the National Office for Serious Fraud, Environmental Crime and Asset Confiscation estimated that in 2020 it "certainly involves a couple of dozen investigations over the past few years" (Nadrous, 2020). An important reason for the lack of clarity and seemingly few cases that proceed to prosecution is that financial intelligence is often a minor part of criminal investigations, perhaps even a single pixel. As no quantitative data are maintained on this, the practical application and added value of financial intelligence – the step *after* dissemination – is difficult to estimate. The scope of dissemination is a worthwhile subject for academic follow-up research.

Here again, pressing concerns can be raised. In contrast to the unusual transactions

21 For case law on terrorist financing, see https://uitspraken.rechtspraak.nl/#zoekverfijn/zt[0][zt]=financiering+van+terrorisme&zt[0][fi]=AlleVelden&zt[0][ft]=Alle+velden&so=Relevance&ps[]=ps1, consulted on June 8, 2021.

database, the suspicious transactions database is accessible well beyond FIU employees. The issue of privacy is thus even more prominent here than in regard to the unusual transactions database, because private information on non-suspects is not only stored and analyzed without the subject's knowledge and consent, it is also shared with a multitude of prosecution and investigative authorities and foreign FIUs. Important to note is the lack of any intervention by a public prosecutor or investigating judge, which means that although transactions in this database are called 'suspicious', in legal terms, the individuals and companies in the database are not suspects. According to the FIU's guidelines for reporting groups, the *Wwft* provides the legal basis for the agency's processing of personal data without permission, without infringing on the requirements of the General Data Protection Regulation (GDPR) (FIU-Nederland, n.d.d). However, as Mouzakiti (2020, p. 23) notes, the different legal frameworks are at odds, and it remains unclear exactly what data protection regulations financial intelligence should adhere to. This is particularly significant in the international context, as in 2020, FIU-the Netherlands exchanged intelligence with 85 foreign FIUs operating in different political, institutional, and constitutional contexts. Is it necessary that private information on non-suspects be made so readily available nationally and internationally? Are the unclear security revenues in terms of combating financial crime in proportion to the impact on personal privacy?

3.7 Conclusion

In the Netherlands, financial surveillance has in recent decades grown into a widespread system that is woven into the very fabric of the economy. Increasingly, payment transactions and spending behavior have become a source of data for investigative and prosecution services. If possible, they use this data to contribute to the prosecution of criminal behavior. FIU-the Netherlands is a crucial pivot in this system because it represents a relatively new type of organization that operates between private and public actors. The FIU depends both on commercial data, which fills the reservoir of its databases, as well as the public services, which use the intelligence. Like the sand that flows through an hourglass, the FIU receives millions of unusual transactions from the 25 mandatory reporting groups. The transactions submitted are categorized as a 'state-secret secret' and assembled in the protected database of unusual transactions. By means of semi-automated analysis and manual investigation, the FIU filters out and selects suspicious transactions, on which additional analysis can be carried out using open and closed sources and a variety of analysis methods. Like the sand flowing into the broad base of the hourglass, the FIU disseminates its intelligence on suspicious transactions to a motley collection of "customers" (FIU-Nederland, 2020, p. 59). This process does not happen without modification of the information as the FIU actively

mediates the transaction information. It disseminates its financial intelligence in two main ways: by making its suspicious transactions database available through BlueView to investigation and prosecution authorities, and by actively entering into bilateral relations and participating in multilateral and international collaborations.

Yet, in the surveillance studies domain, limited attention has been paid to this form of *financial* surveillance. Financial surveillance is not classic Orwellian surveillance, because it is based on private, commercial data (Orwell, 1949). However, the FIU is a public authority that disseminates intelligence to many public investigation authorities. Financial surveillance illustrates that data collection and monitoring need not be focused on certain individuals, or on everyone in a population. Rather, the indicators applied by the FIU steer its data collection in a certain direction, like control buttons that can be turned and tuned, but they do not constitute an all-encompassing 'dragnet'. In addition, financial surveillance demonstrates that monitoring can take place based on intensive collaboration *between* public and private parties. It is a 'fluid' collaboration in the sense that it explores new avenues in which data roams freely in various forms through a chain of actors (Bauman & Lyon, 2013) and is 'translated' in understanding (De Goede, 2018; Latour, 1999). As a legal and operational buffer, the FIU is indispensable in the chain of actors, because it operates as a pivot at the intersection of finance and security, public and private, and national and international. Moreover, it is the only organization that can convert 'raw' transaction information into financial intelligence.

Societies' transition from cash spending to digital transactions makes spending behavior transparent and financial surveillance possible. Yet the questions of *to what extent* and *in what ways* this form of surveillance is feasible have received scant consideration, though these questions are increasingly pressing with the expansion of financial surveillance. To what extent is it ethically justifiable that financial intelligence concerning an individual or entity is declared suspect, investigated, and shared nationally and internationally, without the entity concerned officially being notified and legally named a suspect? Is the privacy violation proportional to the contribution made to investigative and prosecutorial outcomes? What institutional control mechanisms and safeguards are in place and what external control is there on the FIU's activities? These are important questions that should be at the centre of political and policy-related debates.

4

EU FIUs Platform[22]

BOX 4.1 Vantage point: The EU FIUs Platform

This chapter adopts the *EU FIUs Platform* as its vantage point. At the EU FIUs Platform, representatives from 30 European FIUs coordinate cross-border operations and discuss the exchange of expertise and financial intelligence. From this vantage point it becomes possible to discern how geographically dispersed security actors produce shared understandings of financial intelligence. Different ways of constructing financial intelligence encounter each other here, including different understandings of security threats, different ways in which FIUs operate, different legal and institutional frameworks, and different ways of sharing financial intelligence across borders. The chapter, in particular, traces the phrase 'for intelligence purposes', which FIUs often add as a clause when they share intelligence. The chapter examines the interpretive flexibility of this phrase in enabling actors to work together across heterogeneous understandings and the 'flexible scalability' that enables practitioners to assign and navigate several scales at the same time. The chapter concludes that such seemingly trivial elements as this phrase are crucial in enabling the transnational circulation of intelligence.

22 With some minor revisions, this chapter was previously published as Lagerwaard, P. (2020). Flattening the international: Producing financial intelligence through a platform. *Critical Studies on Security*, 8(2), 160–174.

4.1 Introduction

All EU member states have their own FIUs, which collect and analyze large amounts of financial information from private actors such as banks and money transmitters in order to detect illicit financial activities. As financial transactions cross state borders, the FIUs must operate beyond their national jurisdictions and cooperate with foreign counterparts. This raises several challenges. In a pragmatic sense, the FIUs struggle to align their different data sharing models. Some deploy highly advanced software systems, filtering and sending suspicious financial information automatically, while others filter, select, and send each transaction manually. More challenging, however, is the question of how the data is to be utilized once it is in the possession of another FIU. May foreign financial information be forwarded to other domestic partners? Can it be sent to law enforcement authorities or secret services? May foreign information be used as evidence in a court of law?

This chapter investigates how geographically dispersed financial security actors produce and navigate common understandings of data sharing through a joint platform. Drawing on openly accessible meeting minutes, it analyzes ongoing discussions on cross-border financial data sharing within the EU FIUs Platform. The EU FIUs Platform meets periodically in Brussels and comprises representatives of 30 national FIUs,[23] Europol, and the European Commission (DG JUST and DG HOME). In the words of the European Commission, the platform aims to "facilitate cooperation among national FIUs and exchange views on co-operation related issues... relevant to assessing money laundering and terrorist financing risks both on the national and supranational level" (European Commission, 2022). The EU FIUs Platform does not set out to track illicit finance, such as money laundering or terrorism financing, but it serves as the central site in the EU to discuss *how* cross-border tracking practices should be organized.

The chapter utilizes a 'flat ontology' to explore how the production of shared security understandings, including power relations and means of governing therein, can be observed through empirical observation of practices (see, on practices, Adler & Pouliot, 2011; De Goede, 2018, pp. 37–38; Law, 2016). A flat ontology allows observation of how a networked assemblage of actors, both human and non-human, produce and co-constitute persuasive constructs (Latour, 2007, pp. 165–172). A flat ontology draws on empirical induction to unpack how these constructs are maintained and brought into being in everyday practice. Provocatively, Latour (2007, p. 167) claims that the split in the social sciences between local interaction and global context can be presumed "terribly wrong", because it proposes an already existing "framework inside of which interactions are supposed to be nested". Instead, he suggests, inquiry

23 Though not EU members, the FIUs of Iceland, Liechtenstein, and Norway are also members of the EU FIUs Platform. This chapter therefore refers to 30 'EU' participants. Occasionally 31 members are mentioned, because until Brexit, the British FIU was also part of the platform.

should focus on "the very production of place, size and scale", and how in practice these "dimensions are generated and maintained" (ibid., pp. 171–172).

If we ask, following Bueger and Gadinger (2014, p. 65), how we might study "formations of scope – often of 'transnational' or 'global' reach – through a study of something that appears to be as small as practice", then platforms such as the EU FIUs Platform offer an interesting example. This chapter suggests that 'formations of scope' such as the transnational and global – and the more general 'international' – can be studied by observing how these constructs are brought into being and navigated in practice. The EU FIUs Platform includes security actors from across Europe, and their FIUs have bilateral relations around the globe with counterparts and via other 'platformed' institutions. The EU FIUs Platform not only entails physical meetings in Brussels, but it is produced through project teams of groups of FIUs working on specific topics, through detailed minutes of their meetings – and the circulation of these minutes – and through mundane practices, such as meeting schedules, time management, and even the availability of meeting rooms. The EU FIUs Platform offers a window through which to study how formations of scope are being 'done' in practice (Mol, 2002).

This chapter traces the development of one particular EU FIUs project, namely, that aiming to develop a "common understanding" of the three-word phrase "for intelligence purposes" (European Commission, 2015b, p. 5). EU FIUs typically include this phrase as a clause when they share financial data, to indicate how the data may be used by a foreign FIU counterpart. Imposing such a restriction is considered important, as the intelligence shared may contain sensitive information beyond the particular financial transaction deemed suspicious, to also include personal information of the sender and receiver, the bank account, and depending on the FIU, details such as IP addresses. The topic, therefore, warranted the EU FIUs Platform's scrutiny. This led to a project on the particular meaning of the phrase, in regard to concerns such as privacy and encounters with diverse legal jurisdictions (who owns the information and how may it be legally utilized). Whereas some FIUs have to comply with strict national regulations, others operate in more flexible legal contexts, causing particular ways of financial data sharing to collide. As we will observe, the three-word phrase 'for intelligence purposes' operates as a 'boundary object', being both flexible enough to incorporate different interpretations on these issues, while simultaneously enabling the formation of a common, shared understanding (on boundary object, see Star & Griesemer 1989; Fox, 2011; Star, 2010).

After discussing 'flat international relations' in the next section, Section 4.3 then introduces the chapter's data and understanding of the notion of platform. This is followed by two empirical sections. Section 4.4 tracks the phrase 'for intelligence purposes' over a period of a year to observe how it was endowed with *interpretive flexibility*. Section 4.5 then pursues it further beyond the platform and observes its *flexible scalability*. Section 4.6, the conclusion, recapitulates and explores the advantages of the application of a flat ontology.

4.2 Engaging in 'flat IR'

Within international relations (IR) the notion of 'the international' has been thoroughly interrogated. It has, for example, been proposed that "international relations as an intellectual project already assumes that the international is an important – if not paramount – 'pre-established grid of analysis'" (Salter, 2015, p. xvi). The term has been scrutinized for its usefulness and its relation to other concepts such as the 'imperial' (Walker, 2006). Questions have been raised on "what it means to identify the international as a problem, for whom it is a problem, and how it relates to other problems" (Bigo & Walker, 2007, p. 728). This chapter builds on a growing field of IR scholarship which adopts actor-network theory (ANT) approaches (Aradau, 2010; Bellanova, 2017; Best & Walters, 2013; Bosma, 2019; De Goede, 2018; Salter & Walters, 2016). It was first published in 2020 as part of a special issue advancing the conversation between science and technology studies (STS) and IR (see Bellanova, Jacobsen & Monsees, 2020), examining how STS might contribute to IR on such topics as the study of media controversies (Monsees, 2020) and the challenges of producing critique (De Goede, 2020). Drawing on both ANT and STS scholarship, this chapter seeks to conceptually contribute to the question of how to study the international, and how to accommodate the study of scale when researching formations of scope in situated practice.

A flat ontology allows the researcher to understand abstract things, such as scales, not as reified (academic) jargon, but as actively produced constructs having to be continuously stabilized in practice. Scales, for example, are neither a natural given nor offer a static analytical framework (see, e.g., Marston, Jones III & Woodward, 2005). Other abstract notions and grand claims such as 'capitalism', 'neoliberalism', and in our case 'financial intelligence', too, are neither natural givens nor do they offer clear and static analytical frameworks. A flat ontology implies studying how things are actively made to exist in material practice by numerous actors, both human and non-human, and how these actors associate, assemble, and reassemble persuasive constructs (Latour, 2007, pp. 165–172).

Bringing a flat ontology to IR offers two advantages. First, it attributes the rightful weight to the materiality in which things occur, featuring not only humans but also technologies, documents, standardization protocols, and mundane yet vital (inter) mediators, such as meeting rooms, minutes, and time schedules. There is an increasing interest in IR in the role of materiality – the so-called 'material turn' – and exciting research is being done, for example, on the material-discursive practices producing critical infrastructures (Aradau, 2010), the agency and ethics of technologies (see the collection edited by Hoijtink & Leese, 2019), and how 'things' such as bicycles, boats, drones, and even garbage and clocks demonstrate particular ways in which "the international is evoked, enrolled, assembled, and deployed in the material world" (see the collection edited by Salter, 2015, p. xix). What these examples all demonstrate is

the rich level of detail that surfaces when including the material, and the plethora of (non-human) actors that are important to take into consideration. When repositioning the international to where it is made to exist, in everyday practice, we cannot ignore the significance of the things that not only enable, but also produce, manage, and shape the wide scope of topics that IR studies.

Second, a flat ontology allows observation of how common IR concerns, such as power and governance, are not only theoretical contemplations, but can be studied by turning to tiny – yet vital – empirical fragments, such as the clause 'for intelligence purposes' used in FIU exchanges. Doing so shines a light not only on the existence of unequal power relations, stratified scales, hierarchies, and top-down or bottom-up relations, but also acknowledges that these are constructs inherently (re)produced in, and having effects through, situated practices. Of course, the material world is not flat but roughly round and bumped with mountains, lakes, and skyscrapers. Flat is a metaphorical reference and speaks against the tendency to capture the world in generalizing theoretical explanations that often assume static stratified layers (e.g., local/global or micro/macro). The emphasis in ANT and STS turns to how constructs, such as scales, are 'co-produced' (Jasanoff, 2004), 'composed' (Latour, 2010), or 'enacted' (Mol, 2002). However, this dissertation does not concur with Friedman's (2005) interpretation of a flat world as offering an equal, level economic playing field. Instead, a flat ontology, due to its inevitable focus on empirical induction, is understood as allowing a comprehensive address of how unequal relations and stratified hierarchies are made to persistently exist in observable (only materially bumped) practices.

Within the relatively new field of financial security (see, e.g., Amicelle, 2017b; Amicelle & Chaudieu, 2018; Boy, Morris & Santos, 2017; De Goede, 2010, 2017; Wesseling, 2013), ANT and STS approaches have inspired scholars to turn to practice and focus on how seemingly mundane and often routinized dimensions are key to understanding the production of financial security. For instance, by following a single financial transaction through the 'chain of security' (bank → FIU → court), De Goede (2017) shows that financial security actors at different parts of the chain differently ascribe and translate the meaning of the transaction. For transactions to be transportable between security actors, De Goede (ibid., p. 32) observes, they "need to be inscribed in dossiers, analysed, debated and modelled, in order to be rendered intelligible and valid as security facts". Amicelle (2017a) studied a part of this chain, from the bank to the FIU, observing that a shared (but diversely understood) lexicon enabled financial security actors to escape the confines of their own institutional embedment and cooperate across them. Bosma (2019, p. 194) conducted ethnographic research within a major Dutch bank and the financial security field, focusing on what she calls "sites of experimentation", in which new digital security technologies raise ethical and practical dilemmas which challenge security practitioners.

These novel ways of engagement allow new epistemologies and methodologies

within IR to be explored. Yet, they pose new challenges as well (see, e.g., Aradau & Huysmans, 2014; Salter & Mutlu, 2013), and the question of scale remains enduring and imperative (Bueger & Gadinger, 2014, pp. 59–75). Regarding EU financial security, 30 FIUs monitor the financial risks within a population of approximately 500 million EU citizens spread across 10 million square kilometers. How can we flatten the ontology and study such geographically dispersed yet intertwined security phenomena without thinking primarily in terms of national, international, and global and by focusing on only tiny empirical fragments?

This chapter appropriates the concept of the 'boundary object' to investigate how different understandings of financial data sharing find common ground in the EU FIUs Platform (Star & Griesemer, 1989; see also Orsini, Louafi & Morin, 2017). As we will observe, the three-word clause 'for intelligence purposes' has interpretive flexibility: it is "both plastic enough to adapt to local needs..., yet robust enough to maintain a common identity across sites" (Star & Griesemer, 1989, p. 393). As Star and Griesemer (ibid.) show in their study of a zoology museum, shared understandings in this museum needed to align the social worlds of the academic, the patron, the collector, the trapper, and the museum administration. Even 'basic' practices such as collecting, labelling, and describing things (or 'facts') proved far from univocal, and objects with interpretive flexibility were required to generate shared understandings. As we will observe below, the heterogeneous understandings of financial data sharing, similarly, successfully tie together via objects with interpretive flexibility, such as the clause 'for intelligence purposes'.

A frequently posed critique of the concept of boundary object, however, concerns its flexibility regarding scale, since if the scale is flexible, potentially anything could be a boundary object (for a discussion of this topic, see Star, 2010). I argue that this seemingly elusive analytical ability might actually prove invaluable when deploying the concept in IR. The clause allows for 'scalability', I propose, a term deriving from the computer sciences and referring, broadly formulated, to the practice of rescaling applications to (growing or shrinking) sizes and volumes. I do not understand scalability purely as (problems with the) geographical spatial expansion or contraction of certain practices (see Tsing 2015 for this argument), but deploy the term first of all as part of a practice, as a reference to something that is scalable or being scaled. The actors do not bridge or 'jump' scales, but actively (re)produce and stabilize particular constructs of multiple scales with both their feet on the ground. The concept of flexible scalability allows us to acknowledge the multifarious nature of situated scale-making processes, enabling actors to assign and navigate several scales concurrently without being mutually exclusive.

4.3 Studying the EU FIUs Platform

FIUs are designed to collect, analyze, and disseminate suspicious financial transaction data within state boundaries. As they operate primarily within a bordered institutional arrangement, the differences between FIUs are vast: they can be embedded in a ministry or law enforcement agency, be a 'hybrid' of these two, or in exceptional cases – such as the FIU Luxembourg – be a part of the judiciary (EU FIUs Platform, 2016, p. 7; IMF and WB, 2004). EU FIUs differ in human resources (ranging from 13 to 300 employees), financial capacity (from €600,000 to €14 million) and working languages (English is not the continental working language) (EU FIUs Platform, 2016, pp. iii–iv). The EU FIUs Platform thus comprises a heterogeneous group of security practitioners that, similar to the plurality of understandings in the zoology museum (Star & Griesemer, 1989), each have its own particular way of engaging and understanding financial security.

To study this heterogeneous platform this chapter draws on two sources of information. Most important, it draws on the minutes of the EU FIUs Platform meetings from 2014 to 2018. These minutes are publicly available online and have been published since 2014, when the EU FIUs Platform gained its official status as a European Commission Expert Group.[24] The minutes constitute a particularly interesting source of data in light of the secrecy that is commonly part and parcel of security research (see, e.g., De Goede, Bosma & Pallister-Wilkins, 2019). The minutes do not aim to develop policy, but instead describe the actors themselves discussing and reflecting on the construction of policy. The second information source the chapter draws on, in order to contextualize the minutes and comprehend the frequently technical operational debates, is qualitative fieldwork coupled with semi-structured interviews with practitioners involved with the EU FIUs Platform.[25] By engaging with a wide array of financial security practitioners for over two years – in particular with the FIUs – I became acquainted with the relations and interrelations within the field, the sector-specific jargon, and the topics deemed most important by the practitioners themselves (see Boltanski 2011 on this type of engagement).

The EU FIUs Platform is a relatively new player operating at the intersection of national and international regulatory frameworks. Beyond the EU, individual FIUs have their own web of bilateral and multilateral agreements with foreign FIUs. They can be part of international governing bodies, such as the Financial Action Task Force (FATF), which sets global financial intelligence standards, or the Egmont Group, which facilitates global operational cooperation. Notably, both of these organizations are

24 The minutes are available at: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3251, consulted on August 4, 2022. Due to increased calls for EU transparency all expert groups must publish their minutes online.

25 I interviewed six practitioners directly involved with the platform (some involved more directly than others).

governed in a similar fashion to the EU FIUs Platform. In their own words, the FATF is an "intergovernmental body" (FATF, n.d.) and the Egmont Group is a "united body" serving as a "platform" as well (Egmont Group, 2022b).

Informed by platform studies with a focus on digital platforms (Bogost & Montfort, 2009; Gillespie, 2010; Plantin et al., 2018), this chapter zooms in on the importance of these novel types of security platforms involving geographically scattered yet intertwined governmental and intergovernmental actors, including political actors, who periodically meet physically in person. Following Gillespie (2010, p. 350), a platform "suggests a progressive and egalitarian arrangement, promising to support those who stand upon [or are part of] it". Platforms are conceived as an open space for cooperation, in which the organizer, while granted a significant moderating position, is represented as a "mere facilitator, supporter, host" (ibid., p. 353). In our case, the European Commission gains influence by hosting and curating the platform's meetings, thereby holding sway over the amount of deliberation certain topics should or should not receive. Following Plantin et al. (2018, p. 298), platforms such as the EU FIUs Platform can be considered increasingly important within economic and political infrastructures, aligned with the simultaneous movements of "'platformization' of infrastructures and an 'infrastructuralization' of platforms".

The EU FIUs Platform serves as the central location for discussing *how* financial intelligence within the EU should be organized. The representatives of the FIUs and the European Commission gather once every two to four months in a meeting room in Brussels. In addition to these physical meetings, the practitioners collaborate on a number of shared projects (around eight at a time), which are discussed in circulating reports and presented at the physical meetings. The general aim of the EU FIUs Platform, which is to "exchange views on co-operation related issues" (European Commission, 2022), therefore resonates closely with what Barry (2006, p. 239) refers to as a "technological zone"; that is, "a space within which differences between technological practices, procedures and forms have been reduced, or common standards have been established". In our case, however, the platform rather resembles a zone in the making, as common standards regarding, for instance, the sharing of data, are still actively being composed.

The following sections 'visit' meetings of the EU FIUs Platform and observe how the phrase 'for intelligence purposes' developed over a period of a year, and circulated beyond.

4.4 Interpretive flexibility

> The funny thing about 'for intelligence purposes only' is, erm, what is intelligence? (FIU employee, February 26, 2019)

On June 1, 2015, the EU FIUs Platform met in Brussels to discuss the "obstacles to sharing/dissemination of information"' (European Commission, 2015a, p. 7). According to the minutes, the meaning of the phrase 'for intelligence purposes' was unclear, causing misunderstandings between the FIUs when sharing financial data. Due to differing national frameworks, FIUs operated under varying financial sector regulations, legal jurisdictions, privacy codes, and law enforcement institutions. Some FIUs shared financial data and allowed the receiving FIU to use the information as they saw fit, while others were bound by strict national privacy laws. Once the data were shared, however, they might be deployed in ways not foreseen or desired by the FIU that shared it. The receiving FIU might forward the information to domestic partners, such as law enforcement, tax authorities, secret services, or the public prosecution service. As a result, an FIU in one EU country could find its financial data – on a national subject – being used as evidence in a court of law elsewhere in the EU, without having been aware of any intention for such use. As one practitioner tellingly remarked, "[you don't want to] provide information and then the day after, see in the newspaper that the information has been leaked to the press" (FIU employee, February 6, 2020). This raises not only practical challenges around the sharing of data, but also ethical, judicial, and privacy-related concerns.

Responding to a discussion paper by the Hungarian FIU, the first meeting on the topic commenced with the Commission posing several questions: "Does the clause 'information can only be used for intelligence purposes' constitute the only obstacle [to the sharing of financial data]?" "Is use of the clause imposed by national law ([if so,] which provision) or by national fundamental principles? Or is it just used out of habit?" (European Commission, 2015a, p. 7). The clause was considered, at least by the Commission, to be an 'obstacle' to financial data sharing, and it was unclear to the Commission why it played such an important role in sharing practice. Based on these reflections, the meeting agreed to initiate a 'project team' called the "project on obstacles for further dissemination through the 'use for intelligence purposes'" (European Commission, 2015b, p. 3).[26] The 26th meeting of the EU FIUs Platform in October 2015 classified the project as one of the platform's eight core goals.

The new project team conducted an investigation and circulated another discussion paper for the FIUs to reflect on. The team found no international regulations

26 This project team was led by the Hungarian FIU and joined by the FIUs from Austria, Belgium, Cyprus, France, Luxembourg, and Italy (European Commission, 2017c, p. 8).

prohibiting the exchange of information, but observed that some FIUs used the clause because they, in contrast to other FIUs "authorised to provide information for evidentiary purposes", had "less room for flexibility" and could "exclusively exchange information that will not be used as evidence in the course of criminal proceedings or any other sorts of formal procedure" (European Commission, 2015b, p. 5). For an FIU that is not allowed to share financial information to be used as evidence in a foreign court, it can be problematic to share intelligence with a foreign counterpart that *is* legally permitted to do so. Sensitive financial information about a citizen – as mentioned, including more than just the suspicious transaction – might be governed by privacy safeguards in one country, yet when the information is shared with another country that does not adhere to the same standards, the different frameworks might collide in the practice of sharing and using the data. The project team suggested the following:

> Clarity needs to be created on its [the clause's] correct meaning so [as] to avoid undue limitation of the effectiveness of the information exchange between EU FIUs. The aim of this project is to agree on a common understanding (European Commission, 2015b, p. 5).

With this statement, the project team seems to reproduce the academic conceptualization of a boundary object by quite explicitly arguing for the development of a "correct meaning" and "common understanding" (ibid.).

Following the presentation of the Hungarian FIU, the ensuing debate revolved around two interpretations of the findings. The first expressed the opinion of a group of FIUs which argued that a standard clause would have to be developed allowing for "information [to] be used for investigative purposes – thus excluding the use for evidentiary purposes" (European Commission, 2015b, p. 6). However, the Commission "questioned the opportunity for referring to such standard clause", because it "is not legally required in most jurisdictions and leads to ambiguous interpretations" (ibid.). The Commission argued that "at a time where FIU cooperation is high on the political agenda, it seems contradictory that FIUs restrict themselves [in] information exchange by self-imposed limitations" (ibid.). Note that this statement must be understood in the context of the time, as the risks of terrorist financing and attacks like those at Charlie Hebdo and the Bataclan were central in the public psyche. The Commission appears to see the clause as a 'self-imposed limitation'. In response, an FIU representative "noted that the clause allows FIUs to exchange a lot of information quickly". This implies, I would induce, that a standard clause *excluding* use for 'evidentiary purposes' is valuable as it reduces legal constraints and therefore facilitates rapid information sharing in an operational setting, such as during a terrorist attack (ibid.). Apparently, the Commission – setting the agenda – preferred not to use a clause and wanted FIUs to share data quickly nonetheless, whereas the FIUs argued that a clause would reduce legal frictions

and facilitate rapid cooperation. The debate was postponed to the next meeting, and the project team was asked to "come up with further proposals" (ibid.).

The 27th meeting of the EU FIUs Platform, in January 2016, did not focus on cross-border data exchange, as before, but instead pursued the topic of disseminating foreign financial data within the new domestic context. Generally, FIUs do not have executive powers, so when information coming from abroad may prove valuable for enforcement purposes, they would disseminate it to the national agencies endowed with the appropriate executive powers, such as law enforcement. National law enforcement agencies, for their part, might use their national FIU to request foreign financial information, a process often referred to as "diagonal cooperation" (see, e.g., Amicelle and Chaudieu, 2018, pp. 651–652; EU FIUs Platform, 2016, pp. 201–216). These sharing practices imply that data on a person living in Country A, for instance, Belgium, might travel via the national FIU to another FIU in Country B, for instance, Italy, which then sends it on to agencies such as law enforcement, public prosecution, and secret services – and vice versa. At the time, it was impossible for Country A to keep track of how its financial data were conveyed and translated within the EU and within other national contexts. The discussion within the platform, therefore, revolved around which foreign domestic agencies in Country B were allowed to receive the information from Country A, and how these domestic agencies may use the financial data.

The practitioners of the EU FIUs Platform observed that the significance of the debate extended beyond the European context, being likewise relevant to the sharing of information with other FIUs around the globe. According to the minutes, it was "noted that the outcomes of the Project could be valid in [the] global/Egmont dimension and that it also could feed into other mapping projects" (European Commission, 2016a, p. 6). The significance of this remark, and of the Egmont Group itself, will become clearer in the next section when discussing the notion of flexible scalability. The meeting concluded that the Hungarian FIU would prepare and present the final outcomes at the next meeting.

Yet, unexpectedly, the project was not discussed at the next meeting, as it was postponed "due to time constraints" (European Commission, 2016b, p. 8). In addition to thematic discussions, the minutes of the EU FIUs Platform document attention paid to practicalities that, though seemingly minor, are crucial for the EU FIUs Platform to operate and for its practitioners to communicate and assemble. For example, the minutes discuss practicalities such as the availability of rooms (European Commission, 2015b, 2018), the timely circulation of a draft agenda and other discussion documents (European Commission, 2015a, 2015b), and the availability or unavailability of practitioners (European Commission, 2017). Planning the meetings required finding suitable dates (European Commission, 2017a), which should not be subject to change at short notice (European Commission, 2016) or coincide with a national holiday (which is a challenge with 31 national delegations) (European Commission, 2015a). The workings of the

EU FIUs Platform are furthermore grounded in and mediated by the emails sent by the Commission and participants, the laptops on which they send them, the software systems allowing them to do this, and the circulation and discussions of documents such as the minutes. Governing, in everyday practice, is a materially grounded affair, having a substantially pragmatic and important everyday dimension of organizing a meeting. In this particular case, the project had to be postponed because a previous topic, the standardization of reporting formats, took too much time. Quite literally, the production of financial intelligence had to be governed and managed in material practice, and upon failing to do so on this occasion, "it was decided that this point [our project] will be presented at the next meeting of the FIU Platform" (European Commission, 2016b, p. 8).

In June 2016, one year after the project commenced, the Hungarian FIU presented the final conclusions at the 29th meeting. Taking stock of the debate, the project report concluded by suggesting a minimum information threshold for disseminating foreign information to domestic agencies, leaving considerable leeway for the FIUs to decide to which domestic agencies they would disseminate foreign information. However, considering that 17 FIUs were not inclined to give prior consent for the use of their financial information as evidence in a foreign court of law, the project team recommended implementing two phrases, replacing 'use for intelligence purposes'. Thus, when sharing information, an EU FIU should now choose from two phrases:

> A) I give you my prior consent to disseminate the information. The information can be used as evidence in judicial proceedings.
> B) I give you my prior consent to disseminate the information. The information can be used for investigative purposes, but cannot be used as evidence in judicial proceedings (European Commission, 2016c, p. 8).

These two standardized phrases were thus considered to capture the various ways in which financial data was shared, both allowing a common understanding and accommodating the FIUs' different unique sharing practices. These new clauses would safeguard the rapid (and often massive) dissemination of financial security data across EU state borders, as countries that faced legal restrictions could now choose option B and therefore not be unexpectedly faced with their data used in a foreign court of law. The different frameworks and subsequent privacy and legal concerns remained prevalent; yet, as the information could be marked classified, public disclosure (or controversy) could be avoided.

That this new shared understanding was not yet very stable became evident when the "FIU members were asked to endorse the report", and "one delegation expressed a concern regarding the wording of the standard clause B" (European Commission, 2016c, p. 8). This delegation argued that it was unclear what authorities could be considered

as involved in "investigative purposes" (ibid.). It challenged the generic formulation and requested more detail as to what foreign domestic organizations were permitted to receive their shared information. The Hungarian FIU, leading the project, stressed, "this is a non-binding recommendation, whereas some FIUs have [a] very elaborated clause that can still be used" (ibid., p. 9). Yet, the Commission seemed to disagree with the Hungarian representative and "stressed that if there is such recommendation, those FIUs using this type of clause should have an [other] common understanding and standard wording" (ibid.).

By asking for inclusion of a further clarification, the clause seemed to fail to stabilize a shared understanding and lose its interpretive flexibility: it needed to be actively governed. Other FIU delegations did not agree with the objections made by the critical delegate. According to the minutes, they "expressed discomfort" at the idea of the clause being revised, and indicated "that this proposal is coming too late in the process after intensive discussions that were concluded" (ibid., p. 8). The minutes are surprisingly unambiguous in stating that "this proposal was not supported by other FIUs" (ibid.). Power in practice, observably, manifests in these kinds of 'knowledge controversies' (for more on controversies, see Barry, 2012). When the critical note was struck, it became abundantly clear that the previous year of discussions had generated a general consensus successfully integrating the various interpretations and sharing practices into the new clause. Except for one delegation, no further objections were made. According to the minutes:

> The Commission concluded that the project report is mature for adoption without further changes. FIU Platform adopted the report and the recommendation to replace the notion "use for intelligence purposes". No further reservation was made. The Commission congratulated FIU HU [Hungary] for the endorsement of the project report (European Commission, 2016c, p. 9).

4.5 Flexible scalability

> Scale is the actor's own achievement (Latour, 2007, p. 185).

The ability to work across different understandings and develop common ground is one of two key analytical features of a boundary object. The second, as proposed and developed in this chapter, is the notion of 'flexible scalability' to acknowledge the multifarious nature of scale-making processes to denote how actors themselves actively construct and navigate intertwining scales within and between geographically scattered contexts. A boundary object's flexibility regarding scale was originally raised as a point

of critique; for, if an object can hold several scales, it might fail to provide sufficient granularity, that is, level of detail, to deliver analytical clarity (Star, 2010). However, in the current research, this ability might prove invaluable for studying formations of scope by repositioning the making of scale as an empirical inquiry.

Similar to the governing practices of the EU FIUs Platform, the Egmont Group offers a "a platform to securely exchange expertise and financial intelligence to combat money laundering, terrorist financing (ML/TF), and associated predicate offences" (Egmont Group, 2022b). The Egmont Group includes FIUs from around the globe, 166 at the time of this writing, and it facilitates the exchange of financial data as well as the sharing of expertise (ibid.). It is organized into eight regional bodies of FIU clusters. The EU FIUs Platform participants are all part of the 'European I' region, and frequently this regional body meets in Brussels either before or after the EU FIUs Platform meetings. These meetings involve comparable types of participants, with the most important difference being their host. The European Commission hosts the EU FIUs Platform, with a regional focus, and the Egmont Group hosts the European I region, with a global focus. In practice, however, the participants of both operate in a similar context: in a meeting room somewhere in Brussels.

In 2012, the FATF – the 'intergovernmental body' – wrote that "in most countries, STR [suspicious transaction report] information is used *for intelligence purposes* and is not used as evidence in court proceedings" (FATF, 2012, p. 23, emphasis added). The phrase 'for intelligence purposes', it appears, predates the discussions of the EU FIUs Platform and had earlier circulated outside the EU. European FIUs share financial data with and are part of a wider, geographically scattered community of FIUs, using and diffusing similar kinds of terminologies in different contexts. In a similar vein to De Goede's (2017) observation that the meaning of a transaction changes when travelling through the chain of financial security actors, (im)material objects, such as the phrase, circulate, translate, and change meaning from one financial intelligence context to another, within and between diffuse, geographically scattered places.

A practitioner in the EU FIUs Platform, for instance, remarked the following on the EU FIUs' 'use for intelligence purposes' project:

> It has a different origin. It is not initiated solely in the [EU] FIUs Platform, this is a project that comes from Egmont Group of FIUs and it became an FIUs Platform project, or a joint project, because the team members [of the EU FIUs Platform] are very active members of Egmont and felt that what we discuss in Europe is very relevant for the global community, and vice versa (EU FIUs Platform practitioner, May 16, 2019).

The project traced in the previous section, was officially part of the EU FIUs Platform, yet this practitioner indicates that it cannot be demarcated or clearly separated from processes of wider scope. He continued by addressing the relevance of the international community and standardization:

> I mean we don't… only disseminate [suspicious transaction information] within Europe, we share it with the international community as well. And there it would be good if we tried to find a little bit of a global standard as well, when we send information to somebody to have a clear marking on how you can use the information you receive (EU FIUs Platform practitioner, May 16, 2019).

By getting this topic across to the wider FIU community via the Egmont Group, the representatives of the EU FIUs Platform could be said to be 'scaling up'. For instance, the lead of the EU project, the Hungarian FIU, was simultaneously the head of the regional Egmont Group and pursued an active policy to address the clause within the Egmont context.[27] However, the information moves from one space to another, in this case via the Hungarian FIU from one security platform to another. As the practitioner observed, the discussions about the clause, as well as the practitioners themselves, were not confined to one space but moved around. The clause did not travel and translate vertically – from the local to the global – but instead was produced in connected (platformed) practices, crossing and moving through several scales and sites; its movement was grounded – in this case, in Brussels – without being confined to a single scaled strata.

Tracing the phrase further, we can observe its increasing prominence in Egmont Group documents, including the influential and widely used *Operational Guidance for FIU Activities and the Exchange for Information* (Egmont Group, 2017). First published in 2013, these principles entail an attempt to generate a common governance framework for global financial data sharing. Specifically, they aim to formulate shared principles by outlining "generally shared concepts, while allowing necessary flexibility" (ibid, p. 3). Again, we witness a seemingly literal academic description of the intent to produce interpretive flexibility via a boundary object. Noticeably, the first version of this document did not include any reference to the clause 'for intelligence purposes'. In the updated version, published five years later in 2017, one page is devoted to the phrase and its implications (see Figure 4.1) (Egmont Group, 2017). The phrase has become an important consideration in the Egmont context, receiving a prominent position in the operational

27 See, for example, the Egmont Group report Vision and Focus, in which the Europe I region refers to three main priorities, of which the second reads "obstacles for sharing information, dissemination, and further use of information, in particular definition of 'use for intelligence purposes'" (Egmont Group, 2015, p. 32).

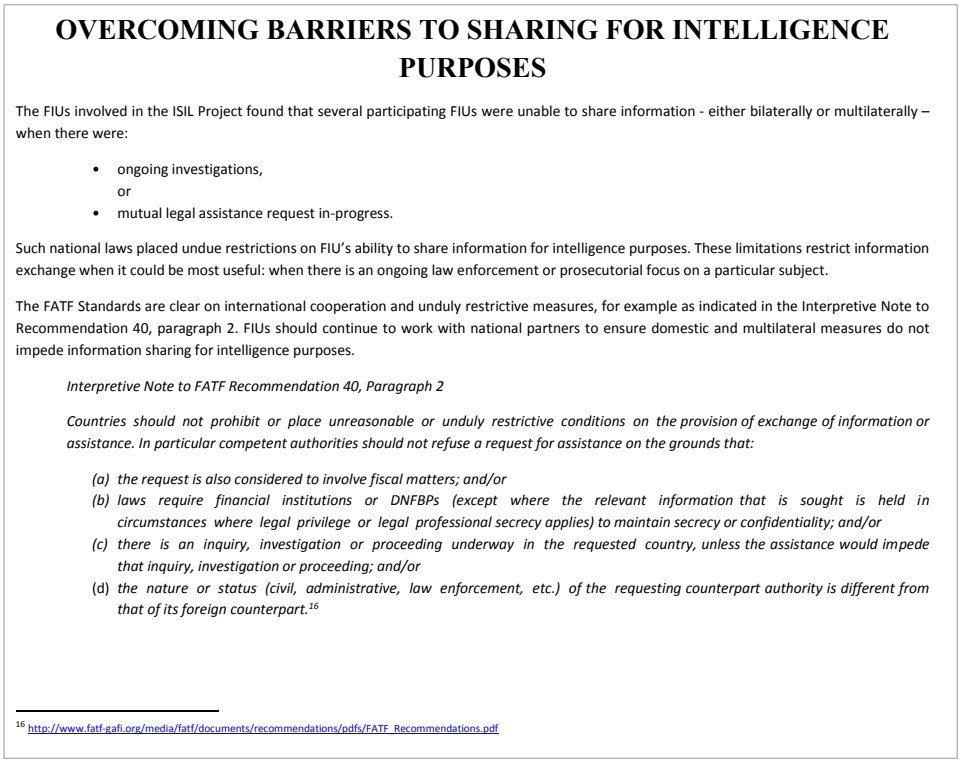
document, which in turn circulates to numerous geographically dispersed FIUs around the globe, not only in the West but also across Asia, Africa, and South America.

Yet, a closer look at the explanation of the phrase reveals several notable differences. First, the verb preceding the phrase *use* in the EU context becomes *sharing* (specifically, the lack thereof) in the Egmont context – thus, the intentions seem reversed. Second, the phrase in the Egmont context exclusively refers to the (financial) fight against ISIL, and suggests that legal questions are barriers that have to be overcome. Third, half of the page refers to a recommendation by the FATF that did not receive particular consideration in the European context. The same three words, 'for intelligence purposes', are being used in a different fashion compared to the discussions in the EU FIUs Platform – even though several similar actors, similar words, and similar meeting rooms are involved.

These variances illustrate that the phrase did not travel uniquely from one space to another (e.g., from the EU → Egmont Group → other national FIUs), nor did it translate into a new, disconnected object. When applying a flat ontology, a level of detail surfaces that obviates the pursuit of causality. Instead, the object and its possibility of including multiple scales seem, in this case, to allow for (multiple) stable meanings across different contexts, enabling the actors to work across them. Both the EU FIUs Platform and Egmont Group meetings occur somewhere in a room in Brussels, occasionally even in the same room (see European Commission, 2019, p. 2). One room, however, is presumed to discuss the global, while the other discusses the regional – though both likely intertwine and incorporate the local, national, and international into a constantly changing mix of shifting scales in both meeting rooms. Amicelle (2017) observes different actors using a similar though differently understood lexicon. In the current case, the actors seem to navigate various interpretations and compositions involving several scales, depending on which side of the hall they assemble. The phrase 'for intelligence purposes' allows for flexible scalability; it can refer to and incorporate various scales concurrently, enabling the actors to produce and navigate scales in grounded practice and engage with topics wide in scope, across situated contexts, and without being mutually exclusive.

As the practitioner noted with regard to the EU FIUs Platform, the debates on how financial data might travel, to which domestic institutions, and how these data may eventually be utilized, are of equal relevance within the Egmont context. In this case, Country A, for instance, Germany, might share domestic (financial) information with a non-EU Country B, for instance, Argentina, which in turn might transmit the information to domestic agencies, such as Argentinian law enforcement, public prosecution, and the secret service. These financial intelligence data sharing cooperations – bilateral as well as multilateral – entail a multitude of scattered 'sites of experimentation' (Bosma 2019), in which the new digital security technologies pose significant ethical and practical challenges for both practitioners and the intertwined political infrastructures of which they

are part. In the current situation, even more than within the EU, it seems impossible for an FIU from Country A to keep track of how its financial data on a person travels and is utilized by counterparts on different continents. Similar to within the EU context, the phrase 'for intelligence purposes', though differently navigated, plays an important role in the global context of financial data sharing. By offering common ground, while being 'plastic' enough to incorporate a plurality of financial security approaches, the phrase facilitates and makes possible the wide circulation of suspicious financial data.



OVERCOMING BARRIERS TO SHARING FOR INTELLIGENCE PURPOSES

The FIUs involved in the ISIL Project found that several participating FIUs were unable to share information - either bilaterally or multilaterally – when there were:

- ongoing investigations,
  or
- mutual legal assistance request in-progress.

Such national laws placed undue restrictions on FIU's ability to share information for intelligence purposes. These limitations restrict information exchange when it could be most useful: when there is an ongoing law enforcement or prosecutorial focus on a particular subject.

The FATF Standards are clear on international cooperation and unduly restrictive measures, for example as indicated in the Interpretive Note to Recommendation 40, paragraph 2. FIUs should continue to work with national partners to ensure domestic and multilateral measures do not impede information sharing for intelligence purposes.

Interpretive Note to FATF Recommendation 40, Paragraph 2

Countries should not prohibit or place unreasonable or unduly restrictive conditions on the provision of exchange of information or assistance. In particular competent authorities should not refuse a request for assistance on the grounds that:

(a) the request is also considered to involve fiscal matters; and/or
(b) laws require financial institutions or DNFBPs (except where the relevant information that is sought is held in circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality; and/or
(c) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding; and/or
(d) *the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart.*[16]

[16] http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

FIGURE 4.1: 'For intelligence purposes' in Egmont Group context. Source: Egmont Group (2017).

4.6 Conclusion

To study the 'grand' question of how geographically scattered financial security actors produce and navigate common understandings of data sharing, this chapter turned to the EU FIUs Platform and observed technical and operational discussions about a 'tiny' – yet key – phrase, as well as how the phrase became institutionalized, how it travelled and was translated within and between institutions, how it circulated in authoritative

documents, and how it might continue to travel and translate – inevitably stopping in the middle of things. What this tiny empirical fragment reveals is not the extent that the 'large' international or global elements constitute a general framework encompassing these types of 'little' practices, but rather how, often abstract, formations of scope, such as scale and the international, are actively made to exist in such, often everyday, material practices, involving not only humans, but also inanimate things, such as rooms, documents, time schedules, and minutes.

By focusing on the key context of the platform where formations of scope are brought into being in situated practice, this chapter demonstrated how financial information sharing around the globe is made possible. The sharing of financial data is being accommodated, even though challenges regarding, for example, colliding legal frameworks, remain prevalent. What the phrase 'for intelligence purposes' ensures is that financial data on a person provided by Country A does not unexpectedly become public or appear as evidence in a court of law in Country B. The phrase is a boundary object incorporating a plurality of approaches, allowing actors to work across these, yet not functioning as a legal or operational safeguard for the exchange of financial information across borders. The clause enables the FIUs to circulate financial data increasingly easily and, given that the data must remain undisclosed, to disseminate it unrestricted to various domestic partners. While within the EU this poses significant challenges, beyond the EU these challenges are even greater, as 166 FIUs scattered across continents share financial information via the Egmont Group.

5

Numbering Practices[28]

BOX 5.1 Vantage point: Numbering practices

Chapter 5 adopts as its vantage point the *numbering practices* of FIUs. Increasingly, FIUs gather data – in particular numbers and statistics – on security threats, such as money laundering and terrorist financing. I found that FIUs gather these data in different ways, through different practices of categorizing, measuring, and standardizing XML formats, and by the use of different software systems. However, despite the different standardizations and the lack of harmonization, the production of numbers and statistics is highly valued by security practitioners around the globe. The numbering practices they use, this chapter shows, serve to provide a technical, depoliticized and technocratic vocabulary that enables FIUs to encounter each other across distance and difference. Without touching on politically sensitive issues, such as what terrorism or terrorist financing actually entails, the numbering practices and associated statistics provide words, concepts, and methods that can be debated, agreed upon, and used to settle disputes. The numbering practices make it possible to develop a transnational space that can be governed, while the urgency of security threats, such as terrorist financing, provides the legitimacy for the sharing of intelligence.

28 A slightly different version of this chapter is currently under review with *Science as Culture*. The full title of the draft article is, "Circulating Knowledge through Disparate Practices: Insights from the Global Pursuit of Terrorist Financing by FIUs".

5.1 Introduction

In 2017, Europol released a report that caused quite a stir in the field of financial intelligence. The report was called *From Suspicion to Action*, and mapped and compared the different practices of FIUs in the EU (Europol, 2017). The report demonstrated that each FIU had a completely different approach to security issues, applying different ways of gathering information, measuring and numbering cases, and sending the resulting financial intelligence to security partners. In response to the report, the European FIUs drafted a collective statement in which they emphasized the significance of the *lack* of harmonization between FIUs, in order to do their job effectively (EU FIUs Platform, 2017, p. 3). They argued that FIUs not only need to work across borders, but that they also need to consider the unique national contexts in which they operate. This rejection of harmonization caused another stir, because harmonization of practices was considered key by Europol and bureaucrats for efficient international and global cooperation.

This controversy touches upon a broader question about the role of harmonization – or standardization, or calibration – in the circulation of knowledge across geographies. To follow suspicious financial transactions across borders, FIUs cooperate with counterparts around the globe, sharing financial intelligence through their joined platform, the Egmont Group. FIUs have to find ways to overcome geographical distance, for example, through digital interactions or physical conferences and meetings, but perhaps more important, they have to find ways to work across their differences. With 166 members, the Egmont Group is characterized by enormous diversity. The members represent countries with fundamentally different political traditions, economic challenges, security issues, and interpretations of human rights and privacy. By adhering to different legal and institutional frameworks, definitions, protocols, and ways of counting and reporting, security issues such as terrorist financing come into existence uniquely within each particular FIU jurisdiction. However, despite their radically different approaches, FIUs do manage to increasingly share financial intelligence around the globe. Exchanges of intelligence rose from 22,532 to 25,301 from 2016 to 2019 (Egmont Group, 2018, 2021a). Is it possible that, in line with the opinion of the FIUs above, the lack of harmonization does not pose an insurmountable hurdle but instead *enables* cross-border financial intelligence?

The question of the role of harmonization, standardization, or calibration of knowledge in the context of information dissemination and cross-border cooperation has been prominent for many years in science and technology studies (STS). In the 1990s, Barry (1993, p. 315) examined the perception within the EU that "harmonization implied that there should be an absolute minimum of national systems of economic and technological regulation". To understand how knowledge is made to travel and exists similarly in different places, STS scholarship has furthermore explored standardization (Epstein, 2009; Lampland & Star, 2009; Porter, 1996), routinization of practices

(Desrosières, 1998), and the "universalization" of metrology standards (Latour, 2007, p. 229). Recent scholarship on data (Leonelli, 2016) and infrastructures (Star, 1999; see also Denis & Pontille, 2019) has furthermore shown that knowledge requires certain (mundane) work, packaging, and maintenance in order to circulate. Leonelli (2016, p. 16) speaks of certain "packaging procedures" of formatting, standardization, and classification that form the "conditions under which data dissemination, integration, and interpretation can or should take place".

Following these literatures, knowledge of 'terrorist financing' should be able to travel across geographies if the ways in which it is brought into being, such as through techniques of statistics and numbering, are calibrated and standardized and able to accommodate different needs across geographically scattered locations. Through what Cakici, Ruppert, and Scheel (2020, p. 2) call "data practices" such as "counting, calculating, cleaning, editing, extrapolating, ignoring, harmonizing" (see also Scheel, Ruppert & Ustek-Spilda, 2019), terrorist financing would materialize relatively similarly in different places, enabling different practitioners around the globe to communicate and work together.

However, this does not seem to be the case with terrorist financing. This security issue travels far and wide and serves as a broad legitimization to share intelligence, but *without* standardized practices of statistics and numbering. The question then is not whether a singular knowledge exists independent of an object – for this discussion I refer to Mol's (2002, pp. 32–33) praxiographic approach – but how and why terrorist financing and its statistics and numbers continue to play such a significant role in processes of global governance, and increasingly so, given the clear absence of shared standardization and calibration of knowledge practices (see, on the role of numbers in global governance, also Hansen & Porter, 2012; Mügge, 2015, 2020; Rocha de Siqueira, 2017; Rose, 1991). This chapter asks, how do FIUs coordinate their operations through disparate knowledge practices of numbering terrorist financing?

To answer that question, this chapter draws on the works of two scholars which, to my knowledge, have only been sparsely included in dialogue, yet in tandem offer a novel way to understand the dissemination of knowledge. They are Annemarie Mol, and specifically, her work on multiplicity (Mol, 2002), and Anna Tsing, and particularly her work on 'friction' (Tsing, 2005). Mol (2002) argues in her research on atherosclerosis in a Dutch hospital that the disease does not exist in a fixed or singular way, but through the entanglement of multiple and different enactments, by surgeons, pathologists, and patients. In a similar fashion, using the notion of multiplicity, this chapter explores how different versions of terrorist financing are brought into being and, more important, how these versions relate globally. Drawing on Tsing (2005), furthermore, the chapter explores what happens when knowledge of terrorist financing is not only decentered and multiple – without a fixed, static essence – but also geographically scattered in a plethora of more or less connected places around the globe. Tsing (2005, p. 4) argues

that global connections can be studied most vividly through "friction", the "awkward, unequal, unstable, and creative qualities of interconnection across difference". It is in those moments when things or people collide and encounter each other, that global connections and coordination become most visible and productive (ibid., p. 5).

Therefore, to understand how knowledge of terrorist financing circulates, this chapter turns to the *coordination* and *encounter* of practices. It argues that some knowledge – for example, of terrorist financing – disseminates and travels far and wide because of its multiplicity and the *absence* of harmonization, standardization, or calibration of practices. In particular, it argues that, despite the different ways of producing numbers and statistics, it is the shared transnational, depoliticized, technocratic, and often highly technical vocabulary of numbering and the production of statistics, that enables FIUs to encounter each other and engage in the coordination of their operations, making the exchange of financial intelligence possible. To run smoothly, the circulation of knowledge on terrorist financing does not depend (necessarily and only) on standardization of practices or their maintenance and repair; rather, it needs to be able to facilitate collision, conflict, discord, and collaboration as well, in order to operate productively. This chapter therefore argues that practices of numbering and statistics do not necessarily serve to align or standardize knowledge to work across distance, in particular in a transnational, global context. Rather, highly technical and technocratic practices of numbering and statistics provide infrastructural substance: a depoliticized vocabulary of shared words, concepts, and methods that can be debated, agreed upon, and used to settle disputes, through which practitioners can encounter each other and coordinate their operations,

The chapter is structured as follows. Section 5.2 brings the work of Mol and Tsing into the conversation and argues that these complementary scholars are key to understanding the dissemination of knowledge regarding terrorist financing. The empirical sections then turn to the security issue of terrorist financing in relation to the global sharing of financial intelligence, with a particular emphasis on the EU. Section 5.3 examines how terrorist financing is brought into existence differently by FIUs, both as an aspiration and as a material reality, leading to disparate practices of numbering and statistics that are difficult to compare. Section 5.4 demonstrates that these different practices, nonetheless, provide a shared transnational vocabulary, the infrastructural substance, to coordinate operations and generate legitimacy on the basis of which FIUs can engage with each other and exchange intelligence.

5.2 Terrorist financing: multiple and decentered

Terrorism and terrorist financing are not fixed, static concepts with clear characteristics (see, e.g., Schmid, 2004; Sorel, 2003). According to Sorel (2003, p. 365), "a substantial number of international conventions have been agreed which deal with various aspects of terrorism, but in all these conventions terrorism is defined in a way that is specific to the subject-matter of the particular convention. No universal definition of terrorism can thus be discerned from them". To use Aristotelian vocabulary, terrorist financing does not have an *essence*, a given state in which it truly exists. In practice, therefore, the threat of terrorism (or terrorism financing) is politically contested, poorly defined, and difficult to know: countries define and view different activities, groups, or persons as terrorists. This chapter argues that it is exactly because of its fluidity, and above all its multiple ways of existence, that knowledge of the security issue of terrorist financing circulates far and wide and makes the exchange of financial intelligence possible.

In doing so, the chapter speaks to the STS literature on the geographical dissemination of knowledge via the harmonization or standardization of practices (see, e.g., Bowker & Star, 2000; Desrosières, 1998; Latour, 1999, 2007; Porter, 1996). Desrosières (1998, p. 9) argues that the reality of statistics derives from the routinized practices that support them, and states that statistics need to be "inscribed in routinized practices that, by providing a stable and widely accepted language to give voice to the debate, help to establish the reality of the picture described" (ibid., p. 1). Porter (1996, p. 28) similarly reasons that for numbers to travel geographically, comparable specifications "must be put into effect at millions of diverse locations, by calibrating millions of instruments and millions of people to the same standard". He writes:

> Since the rules for collecting and manipulating numbers are widely shared, they can easily be transported across oceans and continents and used to coordinate activities or settle disputes.… A highly disciplined discourse helps to produce knowledge independent of the particular people who make it (Porter, 1996, p. ix).

A growing strand of STS literature which focuses on *infrastructures* draws attention to the fact that making knowledge transportable is not necessarily an easy process, but in fact requires substantial effort. Scholarship at the intersection of STS and security has focused on the work required to enable knowledge to circulate through data infrastructures (Bellanova & Glouftsios, 2022; Bernards & Campbell-Verduyn, 2019), financial infrastructures (De Goede, 2021; De Goede & Westermeier, 2022), and critical and political infrastructures (Aradau, 2010; Opitz & Tellmann, 2015). In their study of algorithms in security governance, Bellanova and De Goede (2022, p. 106) set out to "unearth the hard work involved in making data points materialize, and making data

transportable". The study of infrastructures is compelling because it pays attention to the materiality of circulating knowledge and objects, but also to the, often mundane, moments and consequences when an infrastructure breaks down or needs repair and maintenance (Denis & Pontille, 2019; Star, 1999).

Furthermore, recent STS scholarship has pointed out that structured and standardized databases do not, in Porter's (1996, p. ix) words, "produce knowledge independent of the particular people who make it", but in fact require a multiplicity of functions. To understand how 'data journeys', Leonelli (2016, p. 5) studies, "the material, social, and institutional circumstances by which data are packaged and transported across research situations, so as to function as evidence for a variety of knowledge claims". Leonelli (ibid., p. 20) demonstrates that data on model organisms need to be structured in particular ways in order to accommodate and bring together different research traditions. This author's approach to data is closely related to research on "boundary objects" (ibid., p. 20) by Star and Griesemer (1989, p. 393), referring to objects that simultaneously facilitate local needs while also maintaining a "common identity across sites". What is interesting about Leonelli's approach to data circulation, is that the boundary object is not geographically situated – for example, in a museum (Bowker and Griesemar, 1989) – but used to understand how data *journey*, how knowledge travels and is transported to other places in space. However, although accommodating to a multiplicity of functions, the data remain standardized in Leonelli's (2016, p. 5) understanding: "packaged".

Following this line of thought, the concept of terrorist financing would be able to travel across geographies if the ways in which it is brought into being, such as through techniques of statistics and numbering, were calibrated and standardized. By way of similar practices of measuring, calculating, defining, calibrating instruments, and numbering, terrorist financing would exist relatively similarly in different places, making it possible for practitioners from around the globe to communicate and work together. However, this reasoning does not seem to hold. Yes, knowledge of terrorist financing travels around the globe, yet practices of its numbering and statistics are radically different. What makes the security issue of terrorist financing interesting, then, is that knowledge of terrorist financing *does* circulate, but the very *lack* of harmonization of practices seems to be at the heart of global cooperation between FIUs.

To understand the circulation of knowledge on terrorist financing, I draw on the complementary works of Mol (2002) and Tsing (2005). Both Mol and Tsing move away from conventional qualitative social sciences study of 'interpretations' or 'perspectives', because both do not assert that an independent, detached, and static entity exists with inert qualities that can be revealed or exposed (on perspectives, see also Pols, 2005). Whereas Mol (2002) refers to an object (which is multiple), Tsing (2005, p. 1) refers to certain universals (that people aspire to), such as capitalism, science, and politics. Tsing (ibid., p. 7) calls these "universal aspirations", where the universal is not understood as

a singular, uniform, and static rule or "pre-formed law", but rather as something that can be aspired to in different ways in different places. Both Mol and Tsing, then, study the world not by categorizing or examining knowledge that has an overarching, static, and preformed shape, which can be interpreted differently (and these interpretations can then be studied by us researchers), but they study how objects, concepts, and issues manifest in practice differently.

The complementary works of Mol and Tsing, I argue, offer a new way to understand the circulation of certain types of knowledge. To understand the dissemination of terrorist financing (or knowledge about such financing), this chapter is interested in what happens when knowledge is not only multiple and decentered – without a clear essence or fixed state of being – but also geographically scattered in a plethora of more or less connected places. Mol (2014, p. 1) argues that "there are not just many ways of knowing 'an object', but rather many ways of practicing it. Each way of practicing stages … a different version of 'the' object. Hence, it is not 'an object', but more than one. An object multiple". This ontological turn has inspired scholars from diverse fields to study the multiple nature of knowledge, in domains ranging from law (Van Oorschot, 2020) and numbers (Holtrop, 2017), to security issues such as data protection (Bellanova, 2014). Mol (2002) focuses on different "enactments" – suggesting "that in the act, and only then and there, something *is*" (ibid., p. 33, emphasis original) – and how enactments tie together and relate to one another. The word of co-ordination is crucial here because it emphasizes the *co*-efforts of ordering elements in practice. Mol writes:

> As soon as attention shifts to the co-existence of different realities (or logics, or modes of ordering) the question arises as to how these hang together. The term co-ordination is helpful here, since it does not evoke a single, overarching and coherent order in which everything fits just fine and friction-free like the bits and pieces of a mosaic or the components of a watch. Instead, the term co-ordination suggests continuing effort. Tensions live on and gaps must be bridged, hence the need for "co-ordination" (Mol, 2010, p. 264).

Crucially, and distinctively, Mol pays significant attention to non-human actors as part of this co-ordination. As one of the founders of the STS tradition of including non-humans in the analysis (see also Callon, 1984; Latour, 1987), she considers the mediation of mundane elements such as "chairs and tables, food and air, machines and blood" (Mol, 2002, p. 27), asking, "Who does the doing? Events are made to happen by several people and lots of things. Words participate, too. Paperwork. Rooms, buildings… [a]n endless list of heterogeneous elements that can neither be highlighted or left in the background" (ibid., p. 25–26). The object is very real in this sense, grounded in the materiality of

practice, but multiple: different versions tangledly exist. Regarding terrorist financing, we will observe that reports, XML standards, software systems, and ways of numbering and doing statistics actively mediate and bring terrorist financing into existence in practice, differently, yet entwined.

Whereas Mol emphasizes how things 'hang together', Tsing (2005, p. 3) draws particular attention to the "productive friction" generated by certain encounters between universal aspirations. The ethnographic "study of global connections", according to Tsing (2005, p. 5), "shows the grip of encounter: friction. A wheel turns because of its encounter with the surface of the road; spinning in the air it goes nowhere. Rubbing two sticks together produces heat and light; one stick alone is just a stick".

Mol explores the tensions of co-ordination, in particular, in a paper on 'ontological politics'. In it, she writes that "realities may clash at some points, [and] elsewhere the various performances of an object may *collaborate* and even *depend* on one another" (Mol, 1999, p. 83). Tsing, however, focuses not primarily on the continuing effort of these collaborations or dependencies, but on the encounters between aspirations that produce 'heat and light'. In a study of deforestation in Indonesia, she explores how people encounter each other across "distance and difference" (Tsing, 2005, p. 7). In her analysis, she zooms in on "zones of awkward engagement" in order to observe the "productive friction of global connections" (ibid., pp. xi–3). It is in these particular instances that global connections across distance and difference are most visible; but at these times, too, they are most vividly *productive*, because the encounter is pertinent for rearranging a given state of affairs and making (new) arrangements possible. Tsing (2005, p. 5) argues that "as a metaphorical image, friction reminds us that heterogeneous and unequal encounters can lead to new arrangements of culture and power". It is at moments of encounter, therefore, that the coordination of practices becomes most visible and productive.

This chapter argues that knowledge of terrorist financing disseminates and travels far and wide because of its multiple nature and the *lack* of harmonization of practices. The infrastructure facilitating knowledge circulation does not necessarily depend on standardization of practices or their maintenance to make it operate productively. Instead, the circulation of knowledge needs to be able to facilitate collision and discord of disparate practices to bring together diverse practitioners across distance and difference. In this perspective, knowledge practices, such as numbering and statistics, need to be reassessed, somewhat counterintuitively, in particular with respect to the work of Porter (1996) and Desrosières (1998). In the case of terrorist financing, numbering and statistics do not bring knowledge into existence relatively similarly in different places, but make it possible for diverse and dispersed security practitioners to work beyond their national 'appropriation' of terrorist financing and encounter each other (on appropriation, see Schneider, 2003). Through an analysis of knowledge circulation on terrorist financing, I describe terrorist financing as providing a shared transnational vocabulary – that is, the

words, concepts, and methods that can be debated or agreed upon – and as developing a governable space that, in effect, generates legitimacy for practitioners to share privacy-sensitive financial intelligence.

Methodological note

This chapter utilizes on qualitative research conducted between 2016 and 2020, including semi-structured interviews with practitioners at the EU level and from national FIUs, as well as participant observation at practitioner conferences, and desk research. This multi-sited qualitative approach builds on actor-network theory (ANT) and its core assumptions of "localizing the global and distributing the local" (Latour, 2007, p. 219; see also Marcus, 1995). ANT does not distinguish between a 'global context' or 'situated locality', but rather acknowledges that sites are part of an assemblage of associations, including a plethora of mediating and intermediating non-human actors (Latour, 2007; Michael, 2016; Mol, 2010). This chapter relies, in particular, on 11 semi-structured interviews with employees of different FIU departments, of which 8 were recorded.[29] For privacy and data management reasons, places and persons have been anonymized, as described in Chapter 2.[30]

The first empirical section (5.3) returns to the controversy between Europol and the European FIUs, drawing out different ways in which terrorist financing is brought into being. The section commences with the Europol report *From Suspicion to Action*, and more specifically, a graph on the numbers of terrorist finance reports that countries handled (Figure 5.1). It furthermore draws on annual reports from FIUs, combined with the semi-structured interviews set out above, to gain an in-depth understanding of how FIUs construct terrorist financing. The second empirical section (5.4) also draws on the semi-structured interviews, but combines these with international reports from FIUs and intergovernmental organizations such as the FATF. As such, general information from the documents is supplemented by qualitative, in-depth research material.

5.3 The making of numbers and statistics

Figure 5.1 presents a graph from the Europol report *From Suspicion to Action* (2017), showing the numbers of terrorist financing reports that FIUs in the EU received from private reporting entities. It reveals some striking differences. For instance, in 2014 Estonia (EE) processed 2,321 terrorist financing reports. This was almost as many as *all* other EU FIUs combined, while its neighbor, Latvia (LV), processed zero reports that same year. In the UK, more reports were handled than in Germany (DE), France (FR),

29 The data were transcribed and coded with Atlas.ti.

30 Several quotes were translated into English, but the original language is not mentioned to avoid recognition of persons or institutions.

and Italy (IT) combined. The graph thus raises pertinent questions: Do these variations imply that within the EU some countries are facing substantial terrorist threats, while others are not? Or, do the numbers imply that some countries are more effective in detecting flows of terrorist funds, whereas others fail to do so? To understand the different numbers and how they compare, it is crucial to retrace the ways in which terrorist financing is differently constructed in practice by FIUs. In doing so, this section traces how terrorist financing is brought into being differently by FIUs: it exists in multiple ways in different places, not only as an aspiration, but also as a different material reality.

To gather financial intelligence within their jurisdiction, an FIU relies on the reports it receives from private actors, such as from banks and money transmitters. These reports give information on the consumer who made the transaction, the size and nature of the transaction – which can be as small as the purchase of a cup of coffee, or as sizable as the purchase of a house – and the grounds on which the transaction is considered suspicious. These reports can be filed for different reasons: the sum of transferred money may exceed a given threshold,[31] an automated 'red flag' may signal a suspicion,[32] or there may be a subjective reason to suspect illicit economic behavior (see also Amicelle, 2017a; Bosma, 2019). Some countries give private actors the option of filing paper reports and submitting these by regular mail (EU FIUs Platform, 2016, p. 221), but most countries rely on online reporting. Similar to how a scientific 'center of calculation' relies on systematically gathered data that can be inscribed and made to circulate (Latour, 1987), these transaction reports, inscribed with financial intelligence, are a key instrument by which FIUs gather and disseminate financial information on potentially illicit financial activities within their jurisdiction.

31 These thresholds differ per country. For instance, in the Netherlands all cash transactions above €10,000 must be reported, while in other countries such a threshold can be either absent or as high as €32,000 (EU FIUs Platform, 2016, p. 79).

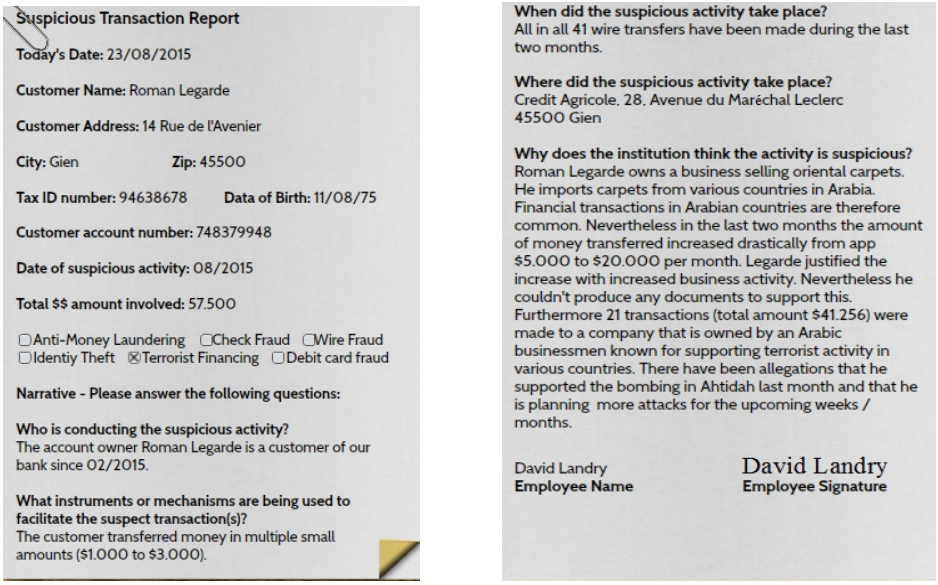
32 A 'red flag' can entail complex automated point systems that classify certain transactions as suspicious (FIU employee, March 12, 2020), but it can also refer to a mundane feature of a transaction, such as involvement of a particular country or region (FIU employee, June 14, 2017).

Country	Total reports filed relating to terrorist financing 2013	Total reports filed relating to terrorist financing 2014	Proportion TF reports 2013	Proportion TF reports 2014
AT	76	61	5.10%	3.65%
BE	126	154	0.55%	0.55%
BG	6	12	0.27%	0.53%
CY	0	0	0.00%	0.00%
CZ	0	0	0.00%	0.00%
DE	208	323	1.09%	1.34%
DK	86	56	1.66%	0.77%
EE	1858	2321	16.55%	20.72%
ES	47	22	1.17%	0.47%
FI	10	13	0.04%	0.06%
FR	200	323	0.73%	0.88%
HR	2	3	0.35%	0.43%
HU	2	4	0.02%	0.04%
IE	586	618	3.84%	3.38%
IT	131	93	0.20%	0.13%
LT	0	0	0.00%	0.00%
LU	47	50	0.96%	0.69%
LV	3	0	0.02%	0.00%
MT	0	0	0.00%	0.00%
RO	1	1	0.02%	0.03%
SE	40	50	0.36%	0.54%
SK	80	79	2.06%	2.01%
SI	7	7	1.17%	1.46%
UK	856	1342	0.27%	0.38%
Total	**4372**	**5532**	**0.53%**	**0.58%**

FIGURE 5.1: Terrorist finance in the EU in 2013–2014. Source: Europol (2017, p. 25).

The nature of these reports differs substantially per FIU. They have different names and abbreviations: some FIUs call them 'suspicious activity reports' (SARs) or 'suspicious transaction reports' (STRs), or they might have names in the respective national languages, such as *penningtvättsrapporter* (Sweden) and *activité déclarative* (France) (see, for an overview, Lagerwaard 2018). Figure 5.2 offers an impression of a transaction report in which a standardized template combines and stabilizes different types of information on 'terrorist financing', including the tick box for this category. This generic example derives from the operational analysis e-learning course for FIU analysts that I completed, and it draws out an important observation: that the financial transactions – in this case several transactions of US $1,000 and $3,000 – are only one element of a terrorist financing report. In fact, the actual transactions do not reveal or signify illicit activity. Different types of information are included in the report in order to assemble a persuasive construct of terrorist financing. The report combines information

that practitioners refer to as 'objective' (e.g., date, address, and sum of suspicious money) and information referred to as 'subjective' (e.g., answers to qualitative questions on why the institution considers the transactions to be suspicious). The report functions as an "inscription device" (De Vries, 2016, pp. 32–33; Latour 1987, pp. 64–68); by combining various types of information on a single page or document, a 'suspicious transaction report' is created which performs a stabilized understanding of that which materializes and can be known and circulated as terrorist financing.



Suspicious Transaction Report

Today's Date: 23/08/2015

Customer Name: Roman Legarde

Customer Address: 14 Rue de l'Avenier

City: Gien **Zip:** 45500

Tax ID number: 94638678 **Data of Birth:** 11/08/75

Customer account number: 748379948

Date of suspicious activity: 08/2015

Total $$ amount involved: 57.500

☐Anti-Money Laundering ☐Check Fraud ☐Wire Fraud
☐Identity Theft ☒Terrorist Financing ☐Debit card fraud

Narrative - Please answer the following questions:

Who is conducting the suspicious activity?
The account owner Roman Legarde is a customer of our bank since 02/2015.

What instruments or mechanisms are being used to facilitate the suspect transaction(s)?
The customer transferred money in multiple small amounts ($1.000 to $3.000).

When did the suspicious activity take place?
All in all 41 wire transfers have been made during the last two months.

Where did the suspicious activity take place?
Credit Agricole, 28, Avenue du Maréchal Leclerc
45500 Gien

Why does the institution think the activity is suspicious?
Roman Legarde owns a business selling oriental carpets. He imports carpets from various countries in Arabia. Financial transactions in Arabian countries are therefore common. Nevertheless in the last two months the amount of money transferred increased drastically from app $5.000 to $20.000 per month. Legarde justified the increase with increased business activity. Nevertheless he couldn't produce any documents to support this. Furthermore 21 transactions (total amount $41.256) were made to a company that is owned by an Arabic businessmen known for supporting terrorist activity in various countries. There have been allegations that he supported the bombing in Ahtidah last month and that he is planning more attacks for the upcoming weeks / months.

David Landry
Employee Name

David Landry
Employee Signature

FIGURE 5.2: Example of a suspicious transaction report from the International Centre for Asset Recovery e-course of the Basel Institute on Governance (2017).

5

In practice, however, each FIU has its own, unique, national, fully or partially automated reporting system by which different types of information are combined. Practitioners themselves often distinguish between two strategies of financial intelligence: focused on emphasizing the earlier-mentioned 'objective' or 'subjective' information. FIUs tend to have focused their analysis processes on either one of these. 'Objective' information consists of stabilized 'factual' information and is often processed by compiling large databases and using quantitative analysis methods. An example is the following reply I received from an FIU employee to my question on whether statistics on terrorist financing, such as those presented in Figure 5.1, are a reflection of the actual security practices of an FIU:

> Not really, no. The number of [reports] reflects the type of obligation for reporting entities [the banks or other private actors].… If the grounds for suspicion which triggered the obligation are very general, very broad, then of course you will have a huge number of inputs by the reporting sector.… If you set a quantitative threshold you may not even be in a situation of suspicion any more. You just have a very objective sort of obligation. And then the number of [reports] might be extremely high depending on how low you set the threshold (FIU employee, February 6, 2020).

Note that this practitioner emphasizes a quantitative threshold above which a transaction automatically becomes suspicious. When this threshold is lowered, for example, from €10,000 to €5,000, private reporting entities have the obligation to classify and report more transactions to the FIU as suspicious. Similarly, if an FIU classifies all transactions involving a particular region as suspicious for terrorist financing, because for example, it is close to the Syrian border and therefore warrants a 'red flag' (FIU employee, June 14, 2017), then the FIU receives more transactions related to terrorism due to this 'objective' obligation. With objectivity, then, practitioners do not refer to the arguments for classifying certain transactions as suspicious, but to an objective criterion set, which can be integrated into the information-gathering process as a threshold or red flag and incorporated into an automated monitoring process that, without (subjective) human interference, automatically labels a transaction as suspicious.

The emphasis on the 'subjective' information, in contrast, is gathered via qualitative methods. For example, a written explanation may be provided of why a transaction is considered suspicious. Consider the following response from an FIU employee to my question about what practitioners understand as the 'risk-based approach':

> An objective system [follows] the rules, and those rules are very easy to apply. In a subjective system you have to rely to a large extent on *fingerspitzengefühl*. So what [this] FIU has always done…, is being very easy and cooperative towards the banks, and asking them to provide us with better and more information.… This has always been the philosophy (FIU employee, August 13, 2019).

The 'philosophy' – or aspiration – of this FIU employee rests on *fingerspitzengefühl*, which can be roughly translated as tacit knowledge combined with gut instinct. An example is provided by the last question in Figure 5.2: Why does the institution think the activity is suspicious? Here, various elements are mentioned – the countries of 'Arabia', a carpet business, the customer's anomalous transaction behavior, the suspicious buyer, the failure to present documentation, and the indirect link to a terrorist attack – all these intertwine

and boil down to a persuasive, though subjective, construct of terrorist financing.

In addition to these aspirations to generate intelligence through either a system of analysis that emphasizes subjective or objective information, there are other, often mundane standardizations and categorizations which bring terrorist financing into existence differently. One obvious example is the national language in which the reporting entities submit their reports. In the EU alone, reports are written in 24 different languages that enable or constrain certain types of definitions and categorizations (EU FIUs Platform, 2016, p. 174). A less visible but vital standardization, furthermore, is the digital format of the report and the specific software used to send it down the national security chain. Each FIU standardizes its reports using a particular XML – eXtensible Markup Language – that translates the information from the human to the computer and vice versa. For example, the tick box option 'category of suspicion' (see Figure 5.2) ascribes a number to each of the illicit activities; for example, money laundering = 1, terrorist financing = 2, and check fraud = 3. Another FIU might follow a different order, for instance, in which terrorist financing = 1, check fraud = 2, and money laundering = 3. This difference in standardization, though seemingly trivial, technologically and materially constructs terrorist financing differently. Furthermore, to transfer these reports down the line of national security actors, FIUs make use of different software programs. Some use protected email systems, with the report provided as a MS Word or PDF file in an attachment, which then has to be uploaded manually within the FIU (FIU employee, January 17, 2019). Others use various automatic standardized online programs, such as a customized version of GoAML.[33]

The varying numbers in Figure 5.1 are a result of the different aspirations and technological and material operations that construct terrorist financing within each jurisdiction. For instance, an FIU that emphasizes the subjective strategy and pays more attention to lengthy descriptions of why a transaction is considered suspicious, would deliver fewer (but qualitatively better) reports. In contrast, an FIU that follows the objective strategy and automatically classifies certain transactions as suspicious due, for instance, to a low threshold or many red flags, would generate more reports of terrorist financing. Looking closer at the extremely high numbers of reports in Estonia (see Figure 5.1), Europol concludes:

> Estonia's high figure is in fact misleading and does not indicate that Estonia is a hotbed for terrorist financing activities. In fact, the Estonian figure reflects the fact that the FIU automatically records transactions to and from certain jurisdictions as terrorist financing (Europol, 2017, p. 24).

33 GoAML is a software product of the United Nations Office on Drugs and Crime for its member states' response to money laundering and terrorist financing. It is available to FIUs to support their work (seehttps://unite.un.org/goaml/ https://unite.un.org/goaml/a, consulted 11 August 2020).

Estonia's high numbers are a result of the automatic labelling of transactions to certain regions – for instance, where terrorist organizations are active – as suspicious. Europol acknowledges that this does not imply that Estonia is a 'hotbed' for terrorist activity. Instead, the high numbers are a consequence of automatic reporting. Some FIUs count each suspicious transaction as one report, while others include dozens of transactions in a single report. This makes comparisons between countries of counts of terrorist financing suspicions difficult, if not impossible.

5.4 Co-ordinating distance and difference

> The fight against terrorist financing must extend across borders and, to this end, FIU-the Netherlands exchanges requests for information (RFIs) with fellow FIUs. In 2019, a total of 50 requests were received from FIUs relating to terrorist financing. In 2019, FIU-the Netherlands sent 34 requests for information to FIUs relating to terrorist financing (FIU-the Netherlands, 2020, p. 46).

Recapitulating, FIUs bring terrorist financing into being differently. They have different universal aspirations concerning to how and what types of objective and subjective information are important, and they use different reports, ways of categorizing, measurements, languages, standardized XML formats, and software systems. The production of knowledge on terrorist financing includes a multitude of national FIUs around the globe, by which disparate knowledge on the same security issue is assembled, mobilized, and constructed differently within each jurisdiction. However, as the quote above suggests, these different ways of producing financial intelligence do not prevent transnational coordination or the exchange of financial intelligence. The quote indicates that, despite the different ways that terrorist financing is produced in practice by FIUs, terrorist financing functions as a perfectly acceptable and legitimate security issue on the basis of which the actual financial intelligence – the reports as exemplified in Figure 5.2 – can be shared with and between FIUs worldwide. This section argues that FIUs' different practices of numbering and statistics do not hinder the transnational exchange of intelligence, but rather, make such exchanges possible, because they provide a shared, depoliticized vocabulary through which FIUs can encounter each other, coordinate, govern their operations, and share privacy-sensitive intelligence.

The substantial variation between FIUs in the numbers of terrorist financing reports they handle and the controversy regarding the desirability of harmonization between Europol and the 31 European FIUs, reveal that despite their many differences, FIUs are remarkably united in their view that harmonization of practices is not something that should be aspired to:

> Harmonizing is maybe an ambiguous word, in a way, because it may mean several different things. We will not be for a fuller harmonization, of course, but certainly for having a common understanding, or a common ground for countries and FIUs to set their information base (FIU employee, February 6, 2020).

By comparing the numbers of FIU reports, Europol makes explicit (and public) that the practices of FIUs concerning terrorist financing are constructed differently across the EU. The report states that "clearly, there is a need to increase the harmonisation of criteria for the collection of statistics, or at least the adoption of transparent standards" (Europol, 2017, p. 39). Europol goes on to argue that "a more far reaching approach is needed to improve the effectiveness of financial intelligence and investigations to tackle terrorism and organised crime" (ibid.). In other words, Europol considers the disparate knowledge practices to be undesirable because they are assumed to be inefficient. In response, the European FIUs drafted a collective critical statement through the EU FIUs Platform. In it, they challenge Europol's argument that harmonization of measurements would make transnational cooperation more efficient. Rather, they argue, a lack of harmonization enables the FIUs to do justice to the national contexts in which they operate:

> It is in fact not possible to come to a meaningful comparison across countries of quantities of STRs [reports,] as the nature, scope and content of such [reports] are profoundly different. These differences derive from a lack of harmonization in EU provisions on the matter, allow a great degree of flexibility across jurisdictions and are at the basis of national peculiarities that have to be individually considered before being able to come to a sensible judgment on effectiveness (EU FIUs Platform, 2017, p. 3).

This quote illustrates why FIUs consider the disparate practices to be crucial. According to the FIUs, the lack of harmonization does not pose a problem, but instead allows FIUs "a great degree of flexibility across jurisdictions". In order to understand effectiveness of financial intelligence, these FIUs argue that the individual peculiarities of FIUs have to be taken into account. These individual peculiarities are important because FIUs simultaneously need to have access to foreign intelligence, but this intelligence also needs to be able to translate back to the national jurisdiction – it needs to 'appropriate' to their jurisdiction, in order to contribute to national security investigations (on appropriation, see Schneider, 2003).

The controversy between Europol and the FIUs demonstrates that practices, such as statistics and numbering, can enable financial intelligence sharing by providing

a common transnational, depoliticized, and technocratic vocabulary that serves as infrastructural substance that exists not only in words but also in methods, protocols, documents, numbers, and other often technocratic and technical practices that give body and shape to transnational intelligence governance and exchange. These do not have to be harmonized, but they do need to be able to facilitate debate, collaboration, and discussion, without touching on the politically sensitive question of what terrorism or terrorist financing actually entails. In order for FIUs to work across their national differences, yet still be able to appropriate knowledge to their national jurisdiction, they need this vocabulary, with which practitioners encounter each other across distance and difference and coordinate and govern their operations.

The FATF provides a telling example. Despite the fact that practitioners know very well that their practices are incomparable (as the report from Europol indicates), the generation of numbers and statistics is increasingly pushed for by this most authoritative intergovernmental organization in the field of financial intelligence. Most countries are members of this intergovernmental organization, and its recommendations are considered influential and enforced through mutual evaluations (Nance, 2018, p. 118). One FATF recommendation deals explicitly with the production of numbers and statistics, as follows:

> **33. Statistics**
> Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT [anti-money laundering/counter-terrorist financing] systems. This should include statistics on the STRs received and disseminated; on money laundering and terrorist financing investigations, assistance or other international requests for cooperation (FATF, 2022, p. 25–26).

This recommendation is considered a vital component of global financial intelligence, as evidenced from the fact that, in 2015, the FATF published an 80-page guidance document on the topic. This document deals solely with AML/CFT-related data and statistics, and includes sections stipulating how FIUs should operationalize processes of "collecting, compiling and presenting AML/CFT data and statistics" and how they should think about "analysing AML/CFT data and statistics" (FATF, 2015, p. 3).

By using complex and often highly technical practices, such as numbering and statistics, FIUs no longer have to debate what terrorist financing actually entails – a shared essence – but instead find these types of often technocratic means to encounter through, as abstracted proxies that provide shared vocabularies. Given the ambiguity and multiplicity of terrorist financing and the politically sensitive question of what it exactly entails, disparate practices, such as of numbering and statistics, provide an

alternative substance on which basis FIUs can encounter each other. Their practices of numbering and statistics offer words, concepts, protocols, terminologies, and methods through which the FIUs can communicate, engage, dispute, negotiate, collaborate, and conflict. It is thus not the resulting statistics or numbers that are significant, but the performance of these together that permits FIUs to generate a complex vocabulary of communication that makes it possible for them to encounter across distance and difference. Figure 5.1, from this angle, *is part* of the encounter, because it produces terrorist financing in Europe. It brings actors together, and it facilitates conversation, conflict and collaborations based on which radically different actors can (or cannot) work together.

Furthermore, this shared vocabulary enables practitioners to render the exchange of global financial intelligence into a governable space. As Barry (1993, p. 316) notes regarding harmonization in the EU, certain technological processes are "directed at establishing this space as a governable entity". Given the diversity of FIUs, the governance of the transnational exchange of intelligence poses a significant challenge, particularly in encapsulating different political traditions, interpretations of security issues, and even differences of human rights and privacy. In its report on data and statistics, the FATF recognizes the challenges that statistics present, in that different definitions and systems make data incomparable (ibid., p. 10). Yet still, the FATF aims to pursue and enforce its 33th recommendation, justifying this pursuit as follows:

> High-quality AML/CFT [anti-money laundering/counter-terrorist financing] statistics can bring several important benefits beyond supporting effectiveness assessments. For example, statistics are a key input for national risk assessments, allowing national authorities to measure threats more accurately and allocate resources accordingly…. Consistent and comprehensive statistics also provide the FATF and other bodies with a more robust quantitative basis for work on global surveillance of the financial system (FATF, 2015, p. 7).

In the case of global intelligence exchange, technological processes seem to provide the tools that enable intergovernmental institutions, such as the FATF and the Egmont Group, to govern global financial intelligence. However, not for the purpose of harmonization, but to make it possible to coordinate operations and provide a "robust quantitative basis for work on global surveillance of the financial system" (FATF, 2015, p. 7) that eventually makes the sharing of intelligence possible.

Furthermore, the practices of numbering and building statistics, while depoliticizing, do not take away the urgency and legitimacy posed by security threats, such as terrorist financing. Because terrorist financing is made tangible and known – in

many different, and conflicting ways – these technocratic practices move the coordination away from debates about the essence and definitions of what terrorist financing is or ought to be, to technocratic issues. However, terrorist financing remains a 'problem space' that, following De Goede (2020, p. 102), "allows innovative modes of financial data-sharing". For example, during an interview in 2018, I raised the topic of the Islamic State (IS) with an FIU practitioner, who responded that this new security issue is "not about terrorism, but about how to share information better. One can use terrorism to get things moving" (FIU employee, March 5, 2018). At a different FIU, a former head of a terrorism department shared a similar perception:

> If I'm being really honest about it, when I was head of [counter-terrorism] financing, I got everything I wanted really fast. When I was head of fraud or head of organized crime, we had to wait ages. But because you got the T-word involved, the terrorist word, stuff gets done, gets done fast (Former head of FIU, May 31, 2018).

Combatting terrorist financing is a driving force based on which new and increased security measures are promoted and implemented (see, e.g., De Goede, 2012, 2020; Lagerwaard, 2020; Vlcek, 2012) and financial intelligence can be shared. It is the urgency of terrorism that constitute sufficient legitimization for the sharing of financial intelligence. Despite the fact that practitioners have moved away from the politically sensitive question of what terrorist financing is to technocratic questions of how it can be known technically, the urgency and legitimacy of the pursuit of terrorist financing remain. The detail that terrorist financing is constructed differently, both as an aspiration and a materiality, does not pose an insurmountable hurdle, then, but instead is instrumental for overcoming difference, because FIUs can encounter each through the depoliticized vocabulary, coordinate their operations, and share privacy-sensitive intelligence that otherwise would not be able to circulate.

5.5 Conclusion

This chapter explored the disparate knowledge practices of terrorist financing through which FIUs coordinate their operations. Drawing in tandem on the work of Mol (2002) and Tsing (2005), it turned to the coordination of practices and to encounters to understand how (knowledge of) terrorist financing circulates and the sharing of financial intelligence around the globe is made possible. The first empirical section examined how terrorist financing is brought into being both as an aspiration and a material reality. FIUs were found to deploy different protocols, software systems, and ways of numbering and counting that produce different versions of terrorist financing, different realities of what

it is and how it can be countered. The second empirical section developed the argument that these disparate practices do not pose an insurmountable hurdle to the sharing of financial intelligence on the topic, but instead make such sharing possible. Practices of numbering and statistics provide a shared transnational, depoliticized, technocratic, and often technical vocabulary through which FIUs encounter one another.

By bringing Mol (2002) and Tsing (2005) into the conversation, this chapter provided a new way to understand the circulation of knowledge. In doing so, the chapter aimed to advance the STS literature focused on the circulation of knowledge and the role of harmonization and standardization (or lack thereof). To understand how knowledge on terrorist financing circulates, the chapter argued that it is insufficient to focus only on how knowledge practices are harmonized (Barry, 1993), routinized (Desrosières, 1998), universalized (Latour, 2007), standardized (Lampland and Star, 2009), and calibrated in millions of places (Porter, 1996), in order to travel from place to place. Furthermore, in the case of terrorist financing, we observed that the bringing together of different practitioners through practices of numbering and statistics does not necessarily involve "boundary objects" (Star & Griesemer, 1989, p. 393) or certain ways of packaging information that "function as evidence for a variety of knowledge claims" (Leonelli, 2016, p. 5). In the case of terrorist financing, practices *are* different and brought into being in unique ways. The shared transnational vocabulary is full of contestation, conflict, disagreements, and collaborations. In fact, this is key to enable knowledge about terrorist financing to circulate between FIUs. Without touching on the political question of what terrorism and terrorist financing means, numbering practices provide FIUs an instrument with which to coordinate their operations, while also maintaining the urgency and legitimacy of the sharing of privacy-sensitive financial intelligence.

5

6

Circuits of Trust[34]

BOX 6.1 Vantage point: Circuits of trust

Chapter 6 adopts *circuits of trust* as its vantage point. Financial intelligence practitioners meet and generate trust through a growing circuit of events, conferences, workshops, seminars, and webinars. This geographically dispersed circuit provides a view of how practitioners develop informal relationships that serve as a basis for the exchange of financial intelligence. The chapter explores trust not just as an abstract notion, but also as a "socio-technical" arrangement that materializes in the circuit, in conversations, documents, and press releases (De Wilde, 2020, p. 564). This vantage point yields key insights regarding the exchange of financial intelligence across distance and difference, because it provides a view of the complex and multifaceted politics of intelligence exchange. Circuits of trust are productive in the sense that they make political stakes evident and exchanges of financial intelligence possible. The chapter examines three practices in particular: the use of trust circuits to navigate a transnational 'legal grey zone'; the use of trust to make intelligence sharing possible (or impossible); and the implicit notions of trustworthiness (or untrustworthiness) at work in the circuit, which lead to inclusion or exclusion. The chapter reflects, in conclusion, on the decision-making powers and autonomy of FIUs, especially with regard to accountability and public oversight. This topic is returned to in the final chapter of this dissertation.

34 A slightly different version of this chapter, co-authored with Marieke de Goede and entitled "In trust we share: The politics of financial intelligence sharing", has been accepted by and is forthcoming in *Economy and Society*.

6.1 Introduction: The Egmont Group

> Trust is an essential component of the Egmont Group. The Egmont Group builds trust among its members by promoting and holding firm on FIUs' integrity, transparency, and accountability. Any abuse of FIU powers compromises trust and is detrimental to the credibility of our global network (Chair of the Egmont Group, Egmont Group, 2021b).

In March 2021, the chair of the Egmont Group of Financial Intelligence Units (FIUs) released a statement addressing "allegations of FIUs misusing their powers to combat ML [money laundering] and TF [terrorist financing]" (Egmont Group, 2021b). The statement acknowledges that certain FIUs misuse their institutional powers by "coercing civil society actors for [their] critiques of current governments in their jurisdictions" (ibid.). FIUs are relatively new security agencies that analyse financial transactions in the context of suspected money laundering or terrorist financing. Banks, but also other financial intermediaries such as money transmitters, are obliged by law to report unusual financial behavior of their customers to the national FIU. The FIU analyses these reports, conducts additional research, and can share the intelligence with the police authorities, investigative services or the prosecution. The Egmont Group provides a global platform for FIUs to cooperate, share expertise and information.

In the Egmont Group statement, it is acknowledged that the considerable powers that FIUs have gained as security actors, can be used to suppress NGOs and/or government-critical groups. As such, it was a rare public acknowledgement of the politics of financial intelligence sharing, and a demonstration that these considerable intelligence-sharing powers can be abused. This chapter takes as a starting point that the politics of financial intelligence sharing are at play not merely in the 'misuse' of FIU powers, but more widely in the ways that FIUs gather, analyze, and share financial intelligence across borders. The statement moreover recognizes and emphasizes *trust* as an "essential component" of the work of FIUs and the ways in which FIUs collaborate and share intelligence. Despite the existence of some international legal frameworks, financial intelligence sharing takes place largely on the basis of mutual trust and personal connections. It is important to draw out more clearly the politics and powers of FIUs and their international cooperation, especially because financial intelligence includes information about individuals who have not been officially charged or formally named suspects in a crime. Crucially, FIUs possess and share extensive personal financial data on citizen-subjects who are unaware that their data are being gathered and circulated. This raises legal, ethical, and privacy concerns.

This chapter maps and analyses the politics of making financial intelligence shareable, with particular emphasis on the practices and circuits of trust. As demonstrated

by Amicelle and Chaudieu (2018), FIUs increasingly share financial intelligence with counterparts around the globe, pushing the legal and practical boundaries of international data sharing for security purposes. This chapter examines the political stakes that arise in practices of sharing intelligence through the Egmont Group. Egmont Group members include countries with questionable reputations concerning human rights, such as Syria, Saudi Arabia, Venezuela, Egypt, and Belarus.[35] As is increasingly recognized in the academic literature, data do not simply 'flow' across institutions and jurisdictions; rather, it takes hard work and complex technical and juridical processes to render data and (personal) information mobile across boundaries (Bellanova & De Goede, 2022; Gitelman & Jackson, 2013). This chapter asks: What are the practical means and networks through which FIU intelligence and data are made sharable?[36] How are investigative files and personal data rendered mobile across jurisdictions, and what are the political challenges and obstacles? What role do informal practices and circuits of trust play in making sensitive financial data and transactions internationally shareable?

This chapter builds on literature in the broad realms of political economy and financial security, to enquire into the practices of transnational financial intelligence sharing, which is an overlooked but particularly important type of data sharing. Literatures in financial surveillance and security indicate that private financial data are increasingly inscribed with the potential to identify suspicious behaviors in the context of crime and terrorism financing (Amicelle, 2011; Gilbert, 2015). FIUs are key in this regard and operate as brokers that receive, analyze, and disseminate financial data within a wider 'chain of security' (De Goede, 2018). In this chain, transaction reports are shared between commercial actors such as banks (Bosma, 2019; Iafolla, 2018), the FIU (Lagerwaard, 2022), to eventually – sometimes – be used as evidence in a court of law (Anwar, 2020). With some important exceptions, including Amicelle and Chaudieu's (2018, p. 650) study of the "devices" and "channels" that FIUs use for transnational cooperation (see also Amicelle & Faravel-Garrigues, 2012), there is a lack of academic study of financial surveillance and of FIU cooperation in particular.

This chapter zooms in on what are termed 'circuits of trust' and the role these play in FIU processes regarding the sharing of intelligence. Results from fieldwork suggest that transnational financial intelligence sharing does not depend only upon technical platforms and structures, but that transnational professional networks and relations of trust are important. This chapter draws on the work of Viviana Zelizer (2006) who has challenged the notion of financial markets as impersonal, and has shown that 'social

35 For all Egmont Group members, see https://egmontgroup.org/members-by-region/, consulted December 1, 2022.

36 By 'data' this chapter understand personal information, including names, addresses, bank account numbers, credit card numbers, IP addresses, social security numbers, and so forth. By 'intelligence' it refers to configured information, such as investigative files, dossiers, SARs, and threat analysis. This separation is not clear-cut, but it helps to distinguish between the information that translates and is inscribed by the FIU and the arguably more 'raw' information they intermediate.

circuits' play a crucial role in the functioning of modern money and credit forms. According to Zelizer (2004, p. 124), "careful observers of [economic] institutions always report the presence, and often the wild profusion, of intimate ties in their midst". Building on the work of Zelizer, this chapter develops the notion of 'circuits of trust' to analyze how trust makes possible the transnational circulation of financial intelligence. Financial intelligence sharing depends on social practices and informal trust relations, and involves mundane political decisions about understandings of which counterparts are 'trustworthy' and 'untrustworthy'.

The chapter is structured as follows. The first two sections discuss literatures on political economy and financial security, and provide more context on the Egmont Group and the challenges of transnational financial data sharing. The bulk of the chapter analyzes three practices of sharing intelligence: on how trust enables FIUs to navigate the legal grey zones of financial intelligence sharing; how circuits of trust materialize and are vital in making intelligence shareable; and how processes of inclusion and exclusion in the circuits connect to political deliberations on the 'trustworthiness' and 'untrustworthiness' of counterparts. The conclusion of the chapter, finally, draws out questions regarding accountability that will be discussed further in the conclusion of the dissertation.

6.2 Trust practices in financial security

In order to examine the role of trust in transnational financial intelligence sharing through the Egmont Group, this section discusses literatures in the broad realms of financial security and political economy. Literatures on 'financial security' demonstrate that financial practices and (state) security are historically and ontologically intertwined (Boy & Gabor, 2019; Langenohl, 2017; De Goede, 2010; Boy, Morris & Santos, 2017). This literature pays attention to the use of finance as a geopolitical tool and "weapon of war" (Gilbert 2015). Within this literature, the study of laws and practices of countering money laundering and terrorism financing (AML/CFT) have become a special focus, because these are so clearly practices where security politics interact with financial interests in complex ways (De Goede, 2012; Amicelle, 2017). In particular, the financial security literature has focused on the everyday, routine practices through which professional groups, like lawyers and bankers, enact regulation and share financial transaction data across public and private spheres (Amicelle & Jacobsen, 2016; Helgesson & Mörth, 2019).

The financial security literature has focused primarily on 'high-tech' modes of data sharing and algorithmic transactions analysis, paying less attention to seemingly 'low-tech' methods, such as personal connections and communications (Bonelli & Ragazzi, 2014). However, as Baird (2017) concludes based on immersive studies of

security fairs, physical encounters of security practitioners are crucial sites where security knowledge is "produced, conveyed, circulated [and] consumed" (Baird, 2017, p. 199; see also Hoijtink, 2019). Similarly, in transnational financial intelligence sharing, 'low-tech' practices, like informal acquaintances, mutual trust, personal meetings and phone calls, seem to be crucial when FIUs cooperate.

Literatures focusing on transnational AML/CFT governance have focused on the increasing prominence of private actors (Liss & Sharman, 2015) and the power of the 'soft law' of transnational organizations (Heng & McDonagh, 2008; Sharman, 2009), but only sparsely on the role of trust. This dissertation suggests that understanding the role of trust in the seemingly high-tech worlds of transnational financial intelligence sharing is important, and can be analysed through what can be called 'circuits of trust,' drawing on Zelizer (2004). The cultural political economy literature has theorized on the role of trust in financial practices, demonstrating that seemingly global and footloose financial markets depend on interpersonal relations and shared cultural practices (Ho, 2009; Pryke, 2010; Siu, 2010). For example, Leyshon and Thrift (1997, p 56) have theorized the cultivation of trust in the City of London that is maintained through informal circuits and ways of dress, and "backed up by abstract expert systems" (Leyshon & Thrift, 1997, p. 56). Trust has become more important – not less so – as financial trading has grown more abstract, technology dependent, and complex (Balázs, 2020; Ho, 2009).

These insights into financial market practices build on a larger sociological literature on trust/distrust (Cook et al., 2005; Searle et al., 2018; Sitkin & Bijlsma-Frankema, 2018). Trust is understood as a human "device" that allows humans to deal with "indeterminacy and interdependence" (Olsen, 2008, p. 2190). Trust has been characterized as a dynamic *reciprocal* process, a "bidirectional phenomenon wherein each party is mutually influenced by the other's cooperation and trust" (Sitkin & Bijlsma-Frankema, 2018, p. 73). De Wilde (2020, p. 2) shows that trust is especially important when economic markets are opaque and economic goods are "multidimensional" and "incommensurable". Trust is a "socio-technical" arrangement, for De Wilde (ibid., p. 564), that is never stable but requires "shared and local work of arranging, modulating and mending relationships". In these conditions, "reliance on others" becomes of key importance as economic participants search for "judgement devices" on what to buy or how to invest (see also Hoffman, 2002; Koole, 2020). Taken together, this literature confirms that trust becomes *more* important as markets and economic processes become more complex, risky and abstract (MacKenzie, 2001).

This dissertation suggests that the politics of financial intelligence sharing can be analyzed through the lens of what can be termed 'circuits of trust'. This approach draws on Zelizer (2004, pp. 124–125), who offered the term "circuits of commerce" to theorize the social relations of "conversation, interchange,… and mutual shaping" that play a key role in practices of commerce and credit. Zelizer (ibid., p. 125) theorizes these intimate ties as "circuits of commerce", understood as "dynamic, meaningful,

incessantly negotiated interactions" between intimate sites such as the household, and formal economic practices and institutions. According to Zelizer (2004, p. 124) "each distinctive social circuit incorporates somewhat different understandings, practices, information, obligations, rights, symbols, and media of exchange" (see also Zelizer, 2006). In other words, a circuit is understood as a bounded social realm with shared practices of meaning-making concerning obligations, worthiness, rights and symbols, and with its own media.

Circuits of trust is a useful term to capture the transnational network of FIUs, as organized through the Egmont Group, which consists both of socio-technical data sharing practices (especially the ESW), and series of formal and informal meetings at which personal contacts are fostered and maintained. This circuit is typified by a large measure of uncertainty concerning trends and methods on terrorism financing and money laundering, which means that participants rely on others to make sense of a complex and uncertain environment. Reliable and shared knowledge concerning suspect profiles and suspicious patterns is often lacking, and there are little to no harmonized reliable indicators (Lagerwaard, 2020; Aradau, 2017). In the face of deep uncertainties over the merits and effectiveness of AML/CFT practices and procedures, participants look to each other to make sense of trends and technologies and to receive and disseminate financial intelligence. This is underscored by the Egmont Group itself calling trust an "essential component" of its operations, the loss of which would be "detrimental to the credibility of the global network" (Egmont Group, 2021b).

6.3 Transnational financial intelligence sharing

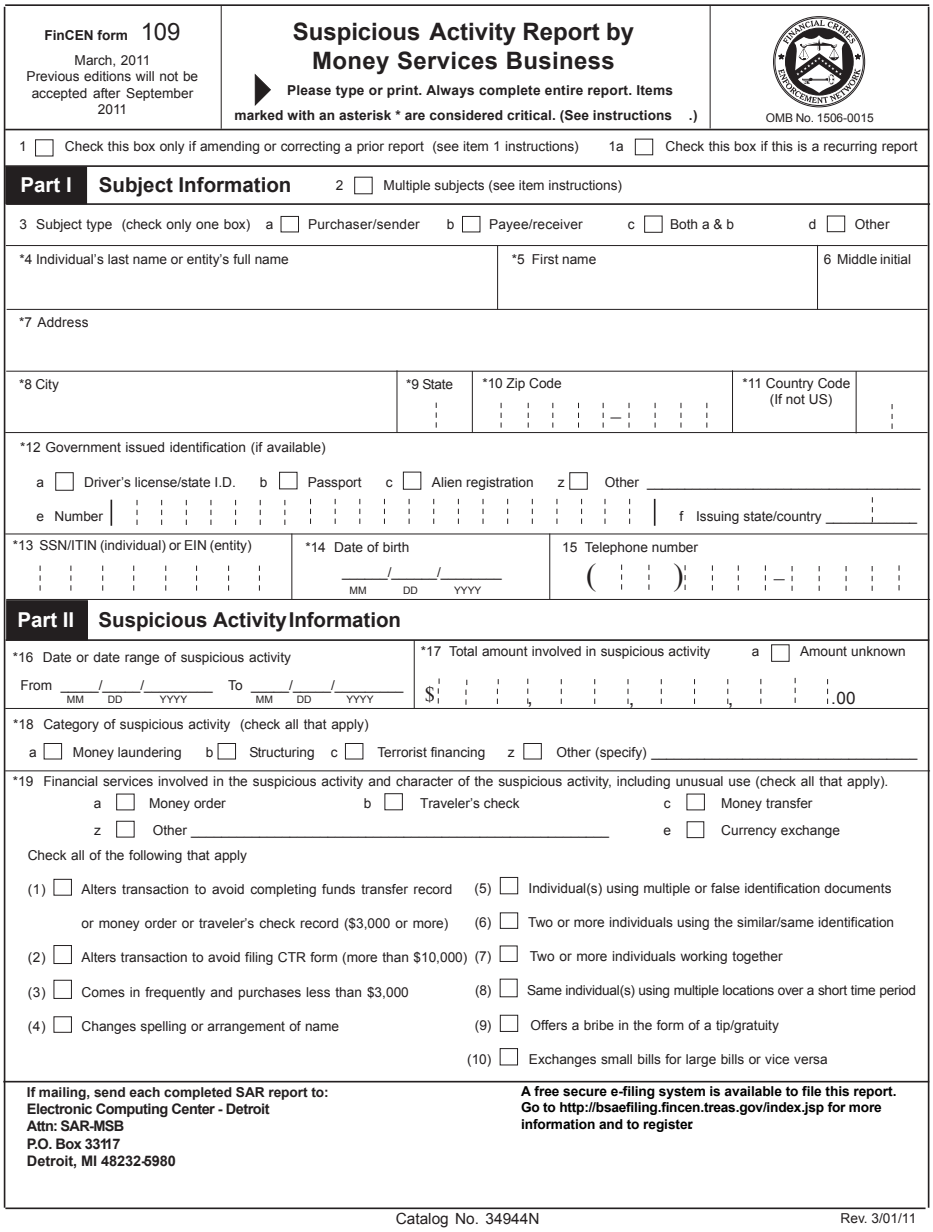
This section introduces the Egmont Group and situates its role in transnational financial intelligence sharing. As a growing literature shows, the ways in which data are made intelligible and rendered sharable across jurisdictions are never neutral but entail complex political choices (Amoore, 2013). Data never simply 'flow' but have to be made mobile across jurisdictions and technical systems and legal regimes (Bellanova & De Goede, 2022). A substantial literature has analyzed systems and practices of 'data-led' security, based on commercial data including airline passenger name records (PNR) and wire transfers (SWIFT) (Amoore, 2013; Bellanova, 2017; Fahey & Curtin, 2014). This literature has analyzed the systems and scale by which commercial airline and financial data are captured and mined by security authorities, raising questions concerning the legal protections and privacy implications of such transnational data sharing (Mitsilegas, 2014). Financial transactions are increasingly considered to yield valuable data points that are intelligible and sharable in the context of security threats (Amoore & De Goede, 2008; Westermeier, 2020). According to Ferrari (2020, p. 522), financial data are particularly privacy-sensitive because they reveal "information about

individuals' activities, purchases and geographical movements," which can be used to derive "sexual orientation, health status, religious and political beliefs".

The reports that commercial financial actors submit to FIUs entail sensitive personal data and narrative descriptions of suspicions. By way of example, Figure 6.1 shows the first page of a SAR report used by FinCEN, the FIU of the US. Part I, 'subject information', includes personal data such as first and last names, address, date of birth, telephone number, and proof of identification (e.g., driving license number). Part II is the suspicious activity information, which includes narrative details on the nature of the suspicion, documentation of the alleged unusual character of the transaction and details about the movement of the transaction.[37]

FIU intelligence sharing differs from existing data-led transnational security programs in that it is less systematic, less 'high tech', and arguably, less visible to date. The Egmont Group network allows a SAR such as in Figure 6.1 to be shared internationally. The Egmont Group is an informal international platform divided into eight regional groupings that align with the regional bodies of the FATF, which is the intergovernmental organization that sets the standards of global financial surveillance (Nance, 2018). The Egmont Group has a largely decentralized structure, its sharing of information, expertise and intelligence is not codified in legal treaties but works through best practice guidance, technical assistance and circuits of trust (Figure 6.2). It was formed in 1995, receiving its name from the location where the 24 founding FIUs had gathered: the Egmont Palace in Brussels, Belgium. The platform has grown to 166 members at the time of writing, with a secretariat based in Ontario, Canada. The organization is funded by annual member contributions (calculated on the basis of GDP and GDP per capita), alongside additional voluntary contributions from members and observers (Egmont, 2019, pp. 27–28). Its highest body is the Heads of FIUs (HoFIUs), composed of the directors of the national FIUs. Below it is the Egmont Committee, which includes a chair and vice-chair positions, which are filled on a rotational basis by the HoFIUs and includes representatives of the eight regional bodies. In addition, the Egmont Group has a learning center, called ECOFEL, which assists FIUs by sharing expertise and best practices.

37 The full SAR can be assessed at https://www.templateroller.com/template/525333/fincen-form-109-suspicious-activity-report-by-money-services-business.html#docpage-3, consulted July 16, 2019.



FinCEN form 109

March, 2011
Previous editions will not be accepted after September 2011

Suspicious Activity Report by Money Services Business

Please type or print. Always complete entire report. Items marked with an asterisk * are considered critical. (See instructions .)

OMB No. 1506-0015

1 ☐ Check this box only if amending or correcting a prior report (see item 1 instructions) 1a ☐ Check this box if this is a recurring report

Part I Subject Information 2 ☐ Multiple subjects (see item instructions)

3 Subject type (check only one box) a ☐ Purchaser/sender b ☐ Payee/receiver c ☐ Both a & b d ☐ Other

*4 Individual's last name or entity's full name | *5 First name | 6 Middle initial

*7 Address

*8 City | *9 State | *10 Zip Code | *11 Country Code (If not US)

*12 Government issued identification (if available)

a ☐ Driver's license/state I.D. b ☐ Passport c ☐ Alien registration z ☐ Other _____

e Number | f Issuing state/country _____

*13 SSN/ITIN (individual) or EIN (entity) | *14 Date of birth MM DD YYYY | 15 Telephone number

Part II Suspicious Activity Information

*16 Date or date range of suspicious activity

From ____/____/____ To ____/____/____ (MM DD YYYY)

*17 Total amount involved in suspicious activity a ☐ Amount unknown

$ .00

*18 Category of suspicious activity (check all that apply)

a ☐ Money laundering b ☐ Structuring c ☐ Terrorist financing z ☐ Other (specify) _____

*19 Financial services involved in the suspicious activity and character of the suspicious activity, including unusual use (check all that apply).

a ☐ Money order b ☐ Traveler's check c ☐ Money transfer

z ☐ Other _____ e ☐ Currency exchange

Check all of the following that apply

(1) ☐ Alters transaction to avoid completing funds transfer record or money order or traveler's check record ($3,000 or more)

(2) ☐ Alters transaction to avoid filing CTR form (more than $10,000)

(3) ☐ Comes in frequently and purchases less than $3,000

(4) ☐ Changes spelling or arrangement of name

(5) ☐ Individual(s) using multiple or false identification documents

(6) ☐ Two or more individuals using the similar/same identification

(7) ☐ Two or more individuals working together

(8) ☐ Same individual(s) using multiple locations over a short time period

(9) ☐ Offers a bribe in the form of a tip/gratuity

(10) ☐ Exchanges small bills for large bills or vice versa

If mailing, send each completed SAR report to:
Electronic Computing Center - Detroit
Attn: SAR-MSB
P.O. Box 33117
Detroit, MI 48232-5980

A free secure e-filing system is available to file this report. Go to http://bsaefiling.fincen.treas.gov/index.jsp for more information and to register

Catalog No. 34944N Rev. 3/01/11

Figure 6.1: FinCEN SAR example. Source: https://www.templateroller.com/template/525333/fincen-form-109-suspicious-activity-report-by-money-services-business.html, consulted May 31, 2022.

According to the Egmont Group, "[the] sharing of financial intelligence is of paramount importance and has become the cornerstone of the international efforts to counter Money Laundering [and] Terrorism Financing" (Egmont Group, 2022b). Egmont Group members commit to sharing intelligence as freely as possible, both "spontaneously", and through cooperation when a foreign FIU makes an information request (Egmont, 2013). The Egmont Secure Web (ESW) is the technology that enables practitioners to engage in everyday communications and to share intelligence via encrypted emails. While the secretariat is based in Ontario, the ESW is hosted by FinCEN, the FIU of the US, and is based in the suburbs of Washington, DC. In 2017–2018, the ESW recorded 22,532 intelligence exchanges between FIU members; in 2019, this number rose to 25,301 exchanges (Egmont Group, 2018, 2021a). Each exchange can entail hundreds of actual reports, including personal data such as bank account numbers, names, addresses, and credit card numbers.

Three Egmont Group documents offer information on how intelligence should be shared. Two of these documents detail specifically the exchange of information: *Operational Guidance for FIU Activities and the Exchange of Information* (Egmont Group, 2017) and *Principles for Information Exchange between FIUs* (Egmont Group, 2013). The Egmont Group Charter (2019), which FIUs *have* to sign when joining, details the shared purpose, definitions, and organizational structure of the Egmont Group . Both the "Charter and the Principles are binding to all members" (Egmont Group, 2019, p. 5). However, in practice the documents leave ample space for interpretation, due to their generic formulation. Moreover, the extent to which these documents are legally binding is questionable because they are not part of any treaty or convention, which means that legal action or international sanctions are not possible against a non-complying country (Amicelle & Chaudieu, 2018, p. 655). We will return to this challenging operational legal situation below.

The Egmont Group encourages members to "check the ESW daily, especially to ensure urgent requests are suitably addressed" (Egmont Group, 2017, p. 4). By keeping the ESW relatively low-tech, the threshold for different types of FIUs to join and share financial intelligence is low. According to some practitioners, the ESW is a very simple system of exchange and can be considered a "glorified email system" (FIU employee, December 26, 2017). Some FIUs make use of highly advanced technologies to gather and analyze data, while others continue to rely mainly on manual processing of (paper) transaction reports, and hardly work with digital reporting. Among these latter are particularly FIUs that operate in cash economies and have few digital transactions available to analyze. By remaining relatively low tech, the ESW allows the diversity of FIUs to connect on an everyday basis.

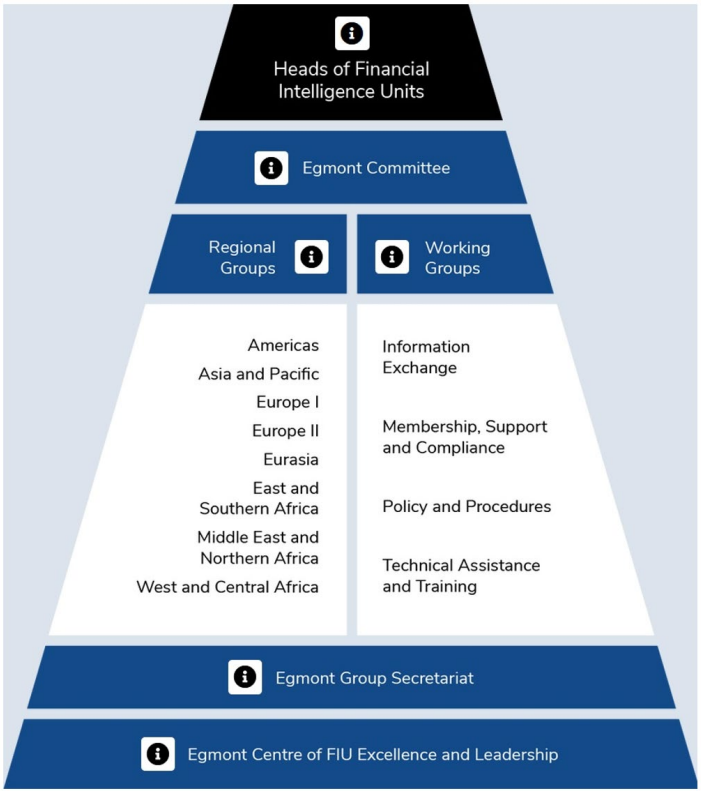


FIGURE 6.2: The Egmont Group's composition. Source: Egmont (2022a).

This chapter asks about the everyday practices and politics of rendering financial intelligence sharing possible, addressing the question how FIUs maintain relationships of trust with counterpart FIUs, even if each must adhere to different regulatory and legal frameworks and have conflicting political stakes and interests. In the following three empirical sections three practices are examined that were inductively identified through fieldwork. First, the international legal agreements and relations that enable FIU data sharing are discussed. These are argued to create 'a legal grey zone' in which circuits of trust play a key role. Second, it is examined how circuits of trust materialize and how they foster informal relations that enable the sharing of sensitive financial data. The focus here is the international conferences and platforms where financial intelligence professionals meet and where interpersonal connections are fostered. Third, the practices of inclusion and exclusion in circuits of trust are discussed, that operate on implicit notions of counterparts' 'trustworthiness' or 'untrustworthiness'. Circuits of trust are not a stable given, according to our analysis, but involve a politics of (dis)trust that might fail or break down.

Our inductive analysis draws on methods of participant observation in the circuit of semi-scientific gatherings on counterterrorist financing and anti-money laundering as panelist, observer, and moderator.[38] It also draws on extensive document analysis of publicly available documents from transnational organizations, including the Egmont Group and national FIUs, which publish annual reports with the numbers of suspicious transaction they receive, analyze, and disseminate. In addition, interviews were conducted in the field of financial intelligence broadly defined, with subjects ranging from bankers to lawyers and regulators, at different institutional levels. Among these, the most important data were derived from 13 interviews with FIU employees.[39] Due to the often sensitive nature of the discussions, comments made by the respondents were anonymized and measures taken to prevent even indirect recognition.

6.4 Trust to navigate the legal grey zone

> FIUs are encouraged to ensure that national legal standards do not inhibit the exchange of information between or among FIUs (Egmont Group, 2017, p. 3).

This section examines the international landscape of legal agreements and relations that form the basis of FIU data sharing. It demonstrates that in intelligence sharing, FIUs operate in a legal grey zone, which makes the role of circuits of trust particularly important. The Egmont Group quote above states that individual FIUs are encouraged to operate at the limits of national law when sharing intelligence with other Egmont Group members. Yet the Egmont Group's 166 member FIUs abide by different national and regional legal frameworks, regarding for instance privacy, data handling, and banking regulations (Mouzakiti, 2020). Importantly, because FIUs operate under such different regimes, shared intelligence might travel from a region with strict privacy or banking regulations, to another region without such regulation, raising the question of which laws and standards then apply to any intelligence that is shared.

Consequently, FIU practitioners face a significant juridical and operational puzzle when sharing intelligence, that derives from a plurality of regulations, guidelines, and laws in effect in different places. On the global stage, the FATF is the most authoritative intergovernmental body. However, the FATF lacks the power to enforce its recommendations nationally. Instead, it relies on regional bodies and a system of

38 Events attended included the Thirty-Sixth International Symposium on Economic Crime, 'Unexplained Wealth – Whose Business?', September 2-9, 2018; the Chatham House, 'Illicit Financial Flows', November 19, 2018; and the ACAMS, 'Fourteenth Annual Anti-Money Laundering and Financial Crime Conference to Address Global Financial Crime Threats', May 31-June 1, 2018.

39 The data were coded and analyzed using Atlas.ti and securely stored with VeraCrypt. See also Chapter 2.

mutual evaluations (Nance, 2018). This results in countries interpreting and translating the FATF recommendations differently. For instance, the EU has translated the FATF recommendations into its Anti-Money Laundering Directive (AMLD), which has been adjusted multiple times since its first implementation in 1991 and is currently in its sixth version. An EU directive is binding in its goal, yet countries are allowed to decide how the goal is to be translated into national legislation and accomplished. Countries around the world translate global and regional frameworks into legislation that might differ in terms of banking regulations, privacy, data sharing, and even issues of human rights. In sum, countries implement loosely defined 'recommendations' (FATF, 2022) or 'principles' (Egmont Group, 2017), which are not legally binding in their own jurisdictions. Transnational cooperation to counter terrorist financing and money laundering is therefore marked by informal global governance arrangements.

FIUs navigate this sensitive legal grey zone by relying on circuits of trust, and loosely structured informal relations. The importance of trust is officially drafted as part of the Egmont Group Charter, which prescribes that "effective international co-operation between and among FIUs must be based on a foundation of mutual trust" (Egmont Group, 2019, p. 4; see also the Egmont Principles, 2013, p. 3). As discussed, the international governance of the Egmont Group is in the hands of the HoFIUs group:

> The Heads of FIU (HoFIU) are the Egmont Group's main governing body. The HoFIU make consensus-driven decisions on matters affecting membership, structure, budget, and key principles. The HoFIU communicate regularly through the Egmont Secure Web and meet at least once a year during the Annual Egmont Group Plenary meeting (Egmont Group, 2022a).

The international relations connecting HoFIUs and the governance of the Egmont Group are partly encoded in official documents, yet there are no binding regulations that obligate HoFIUs to participate in the Egmont Group, let alone to share their intelligence. The fundament of international cooperation is personal acquaintanceship – and consensus – among the HoFIUs.

Circuits of trust are fostered through the personal connections between HoFIUs and their closely connected personnel working on foreign affairs. The actual sharing of intelligence, too, takes place on the basis of informal agreements rather than legal procedures. This dissertation found through fieldwork that instead of formal mutual legal assistance requests, often FIUs first shared their intelligence informally, requesting formal permission for its use only afterwards, if the data appeared to be valuable. An example is provided by the comment below, made by a former HoFIU in response to a question on the importance of trust:

> [Trust is important b]ecause of the informal nature of contacts between FIUs. So it's an intelligence based [system]. It's not, it doesn't involve the mutual legal system..… [For] FIUs, the rules are… more lax, I would say. It's for intelligence purposes only. So if there's a real investigation afterwards, then there will be MLA [mutual legal assistance] anyway, so everything will be checked. But for now, just queries like "do you know this person" and "is there information about this person". So, sometimes it's exchanging STRs or sensitive information, and sometimes it's just assisting with even open source information (Former HoFIU, September 6, 2018).

This suggests that in the case of FIUs, the process of using foreign intelligence legally for domestic investigations or in a court of law is reversed. First, the intelligence is shared on the basis of trust and in the confidence that it will be used 'for intelligence purposes only', thus remaining behind closed FIU doors. If it proves to be important, for instance as key evidence in a criminal investigation, then the official legal permission is requested from the counterpart FIU (FIU employee, January 17, 2019).

Like the FATF, the Egmont Group lacks the 'hard' power to oblige (Ho)FIUs to share intelligence, meaning that in practice national FIUs remain in full possession of their own data, including their suspicious transaction reports (SARs). This leaves space for FIUs to independently navigate and decide when, how, and what kind of financial intelligence they share with foreign counterparts. It is precisely in the context of the legal grey zone, that the circuits of trust are built, maintained, and mobilized, so as to navigate the plurality of possibly conflicting legal frameworks. Trust in the counterpart provides some form of informal, unofficial safeguard against misuse, that is not always warranted, as will be observed below. Moreover, the significant role of trust in navigating the legal grey zone and bringing about global sharing of financial intelligence is widely acknowledged by the practitioners themselves. As the Head of the Egmont Group stated in response to the allegation that FIUs had misused their powers "These deeply concerning allegations pertain to FIUs limiting or coercing civil society actors for their work and critiques of current governments in their jurisdictions … Any abuse of FIU powers compromises trust and is detrimental to the credibility of our global network" (quoted in Vedrenne, 2021).

6.5 Making intelligence shareable through trust

The previous section argued that FIUs operate in a legal grey zone and face a juridical puzzle, which leaves them space to independently decide what kind of intelligence they share with counterparts. This section explores how the circuit of trust materializes in practice via various types of events. Following De Wilde (2020), this chapter understand trust not just as a social bond but as a 'socio-technical' arrangement that requires practical work and material platforms. With regard to terrorism financing and money laundering, there is a fast growing circuit of events, conferences, workshops, seminars, webinars, and symposia at which financial professionals and security practitioners meet and interact. These events range from the annual Egmont Group Plenary, to private events, such as the Association of Certified Anti-Money Laundering Specialists (ACAMS), and academic events, such as the Cambridge International Symposium on Economic Crime. Workshops and webinars have titles such as 'Illicit Financial Flows: Assessing the Need for New Approaches' and 'Unexplained Wealth: Whose Business?' Participating in these events is costly. The ACAMS Annual conference cost US $1,085 (public sector rate) and the Cambridge Symposium on Economic Crime cost UK £2,400, to which expenditures for accommodation and dinners must be added. To some extent then, the events themselves generate the circuit in a material infrastructural sense; they provide a sense of exclusiveness of the circuit, as well as a shared 'ingroup' feeling.

The Cambridge Symposium is an example of a large event where trust is fostered across a wide spectrum of financial intelligence actors. The conference is organized by the University of Cambridge and attended by more than 2,000 participants from over 100 countries.[40] Over the course of eight days it provides 120 sessions – mainly workshops and individual speakers – and gathers more than 650 experts from the financial intelligence field. Beyond FIU employees, participants include bankers, law enforcement officials, law firms, representatives of nongovernmental organizations, consulting firms, public prosecution services, politicians, secret services, and (global) governance agencies, such as the FATF. Trust is not an official part of the program, but in practice, speakers and the workshops recurrently signal the importance of trusting fellow practitioners. Trust building was put into practice during networking opportunities, including cocktail parties and diners, at which attendees exchanged business cards and reconnected with acquaintances.

The importance of such, often physical, gatherings in generating trust among practitioners is widely acknowledged. Consider, for instance, the following conversation with a former HoFIU, offering an apt illustration of the significance of the Egmont Plenary:

> Respondent: Well the Egmont Group is fantastic. It's the best cocktail party in town.

40 See https://www.crimesymposium.org/, consulted July 16, 2021.

> Interviewer: At the moment or before?
>
> Respondent: It always has been, it always will be. Because they meet in the most exotic places.… And for many years there wasn't much coming out of Egmont. I think now it is quite a bit more substance. But even assuming there's no substance it's just a good cocktail party. It has a lot of value because you meet people, shake hands, you look people in the eye, and then, trust is gained (Former HoFIU, September 6, 2018).

This former HoFIU emphasized the importance of 'looking someone in the eye' to generate a sense of trust with other FIU heads and professionals. Indeed, the making of shareable intelligence is more than just a pragmatic exercise of implementing technological devices and legislative frameworks. Rather, it is built during these types of mundane occasions and interactions. Informalities are key to the sharing of financial intelligence, as this former HoFIU explained further:

> You go to other countries, for me to go to the Netherlands,[41] I don't know how to go to the company registry of Netherlands. It's a different language. You call the FIU, "Can you help me?" "Yes, sure",… "by the way we also have two [SARs], and we have some information". So this very informal way actually turns out to be very, very useful.… Egmont Group can be criticized for being a cocktail party, not doing much, but even as such, I claim, many cases I can remember,… I could call… and I can say "Hey, George, how are you doing? Remember, we had fun together last week? Can you help me on this case? It's really important." "Sure, I can look into it" (Former HoFIU, September 6, 2018).

The relationships of trust that are generated at these types of conferences, often develop on the basis of reciprocity. According to Cook, Hardin, and Levi (2005, p. 2), "a trust relation emerges out of mutual interdependence and the knowledge developed over time of reciprocal trustworthiness". Given that FIUs have contradictory interests – being simultaneously dependent on the intelligence of others while seeking to protect their own sensitive data – reciprocity becomes an important concept around which delicate political decisions are made. The Egmont Charter, for instance, reads that "[a]ll members foster the widest possible co-operation and exchange of information with other Egmont Group

41 This respondent used the Netherlands as a fictional example because the interviewer was from that country.

FIUs on the basis of reciprocity or mutual agreement" (Egmont Group, 2019, p. 8).

How reciprocity plays out in practice is demonstrated by the following response of another HoFIU when asked whether they exchanged data *differently* with FIUs outside of the EU:

> Yes, yes, of course we make, well, of course we do not carry out extensive analysis [of the other FIUs] because the membership to the Egmont Group somehow provides reassurance. But we have conditions in our law, for example, about confidentiality and reciprocity, which are very common conditions worldwide. So we can only provide information to FIUs that are, you know, that commit to keep that information confidential and abide by the conditions that we might indicate (FIU employee, February 6, 2020).

This interviewee considered membership of the Egmont Group as providing reassurance, and also mentioned that reciprocity between FIUs does not necessarily refer to an equal exchange of data – a balanced or equal 'weight' or 'worth' of the intelligence exchange – but rather to the extent that the FIUs trust each other to share sensitive data. Practices of trust and reciprocity provide reassurance that in the absence of a shared legal framework the intelligence will be handled with care and confidentiality. Overton (1999, p. 40) also observes that reciprocity does not necessarily mean an equal relationship of trust; it may involve unequal relationships in which some parties have more influence than others.

FIUs in countries with questionable reputations concerning human rights are members of the Egmont Group and can become part of the circuit of trust, as will be analyzed in the next section. Indeed, these FIUs are considered important because they have access to valuable intelligence from their respective jurisdictions, which otherwise would be difficult or impossible to acquire. From an intelligence perspective, it is beneficial to have as many FIUs as possible as part of the circuit, as this expands the global pool of accessible intelligence. Take for instance the following quote from an FIU employee:

> [W]e used to say in Egmont… it is better to have bad FIUs on board, than have them outside the system. For example, if I may refer to some FIUs, some offshore FIUs, sometimes they might provide valuable information… which we are investigating and which may have accounts for companies offshore… [A]lthough this may be a little sketchy, still it is very important, for example, for us and for prosecutors in [country] to understand if there is an account in, say, the Cayman Islands (FIU employee, February 6, 2020).

Being part of the transnational circuit of trust is therefore key for an individual FIU to gain access to and tap into a wealth of data from around the globe. However, to achieve this, the FIU must become part of the circuit of trust and join the growing circuit of events, workshops, and other, often physical, gatherings and relations. Practitioners such as HoFIUs need to be part of the transnational circuit. They need to be present to look other practitioners 'in the eye', and engage in reciprocal relations of data sharing. This includes FIUs that "may be a little sketchy" (ibid.).

6.6 Inclusion and exclusion: The politics of (dis) trust

The previous section analyzed how trust materializes in practice as a fundamental component of the global operations of the Egmont Group. This section shows that this also involves a delicate politics of (dis)trust, especially because FIUs have considerable autonomy to independently decide with whom (not) to share financial intelligence. It argues that this political dimension of transnational financial intelligence sharing involves a process of inclusion and exclusion. Following Zelizer (2004, p. 125), economic circuits "imply the presence of an institutional structure that reinforces credit, trust, and reciprocity". This means that a circuit of trust requires work to operate and maintain. Informal circuits are not stable and static, but are prone to blockages and delays, and may even break down (see also Bellanova & De Goede, 2022). This section focuses on the politics of sharing financial intelligence through circuits of trust, and the concomitant importance of trustworthiness/untrustworthiness.

The autonomous nature of FIUs grants them considerable power to independently decide with whom to share information, without governmental interference. In fact, FIUs are granted this autonomy in order to safeguard against governmental interference and the potential misuse of financial intelligence by, for instance, autocratic regimes. For instance, the 28th FATF recommendation reads as follows:

> The FIU should be able to obtain and deploy the resources needed to carry out its functions, on an individual or routine basis, free from any undue political, government or industry influence or interference, which might compromise its operational independence (FATF, 2020, p. 103).

On the one hand, this independence functions as a safeguard for when FIUs share intelligence with "sketchy" counterparts, because FIUs from questionable countries are expected to be separated from government and therefore protected against external interference. It is for this reason that FIUs are often viewed by the wider financial security

field as peculiar organizations, in that they tend to be more loyal to each other than to their respective governments (Think tank practitioner, October 16, 2020). On the other hand, this principle of operational independence and autonomy vests considerable political power and responsibility in the hands of the FIUs, that is not always warranted.

As mentioned in the introduction, the Egmont Group recently issued a warning about potential abuses of FIU power (Egmont Group, 2021b). This warning referred to recent cases in which FIUs allegedly abused their powers. Two of these cases are relatively well documented. The first case concerns the FIU of Uganda, the Financial Intelligence Authority (FIA). In December 2020, a few months before the country's elections, FIA ordered the freezing of four bank accounts belonging to civil society actors that were "involved in good governance and election observation in the country" (Draku, 2020). FIA has the authority to freeze bank accounts – a power not shared by all FIUs. It froze, among others, the accounts of the National NGO Forum, which is an umbrella organization including more than 650 organizations (Issa, 2021). Following a political controversy in which FIA was accused of misusing the money laundering and counterterrorist financing regulations for the political purposes of the ruling party, and following pressure by the US and EU (The Independent, 2021), FIA reversed its decision and released the accounts. However, this occurred only in February 2021, after the elections (Kazibwe, 2021). This example demonstrates that an FIU, despite its (desired) autonomy and independence, can be mobilized by governments for coercion of civil society in political struggles.

A second example concerns the FIU of Serbia, called the Administration for the Prevention of Money Laundering (APML). In this case, intelligence was shared by the FIU for questionable purposes. Specifically, in July 2020, APML requested commercial banks to provide detailed information on Serbian civil society and media subjects, basing the request on Serbia's Law on the Prevention of Money Laundering and the Financing of Terrorism. In response, 270 civil society actors and media representatives issued a joint statement proclaiming that they would "not give up the fight for a democratic and free Serbia".[42] The UN Human Rights Office warned that "Serbia's anti-terrorism laws [are] being used to target and curb work of NGOs". Even the FATF responded, stating that it "shares the concerns regarding the allegations that Serbia misused its Law… with the aim to restrict or coerce civil society actors for their work and criticism of the government" (FATF, 2020b). In this case, furthermore, the Serbian government explicitly acknowledged that the APML was actively gathering information from foreign FIUs on national subjects. It stated that "in the course of its work, APML has collected information on the cases which involved government officials, including ministers currently in office, using its powers to obtain information from foreign FIUs" (Permanent

42 See, for the statement, https://www.gradjanske.org/en/civil-society-and-media-will-not-give-up-the-fight-for-a-democratic-and-free-serbia/, consulted July 17, 2021.

Mission of the Republic of Serbia, 2020). Information that is shared between FIUs, this example shows, can be put to use for purposes that do not adhere to the standards of the FIU that initially provided the information, possibly conflicting with privacy standards but also, potentially, human rights.

Both examples demonstrate that individual FIUs make delicate political decisions about with whom to engage in reciprocal relations and data sharing, because these data might become 'complicit' in domestic political decisions and the undermining of civil society. One FIU employee noted that if they determined that another FIU had been deployed for domestic political purposes, they would stop sharing data with the FIU: it would be excluded on the basis of distrust. Such a breakdown of trust was described as follows:

> There have been cases of leaks of information, of very confidential information, provided on suspicious cases and on individuals which were leaked in foreign countries for political purposes, for example, because the guy which was being analyzed or investigated was the former prime minister or the current prime minister. Therefore, the FIU was actually used as a conduit to, you know, in the context of political struggles there. You provided information, and then the day after you saw in the newspaper that the information had been leaked to the press. So [it] is… very unfortunate to have the trust compromised. I mean, of course, next time you won't accept to, you know, share information with that FIU. So that is why trust is essential (FIU employee, February 6, 2020).

If trust breaks down because an FIU has used the shared information for domestic political purposes, then the exchange of financial intelligence can come to a halt. This has less to do with technicalities, legal regulations or whether the Egmont Charter has or has not been signed, and more to do with the everyday practice and politics of sharing financial information through circuits of trust. As the quote above shows, the politics of trust or distrust do not necessarily relate to whether an FIU is located in a county where human rights abuses take place, but relate to the question of whether an FIU is considered 'a bad apple' and whether it has taken adequate care of the sensitive financial information it has been given access to.

The uneasy inclusion of the Syrian FIU under the Assad regime in the transnational circuit of trust presents a final interesting example of how delicate this politics of (dis) trust and inclusion/exclusion is. Syria has been an Egmont Group member since 2007, and has remained included, to different degrees, in the FIU circuit of trust during the

civil war.[43] While the regime's use of chemical weapons on its own population led to the severance of diplomatic relations between European countries and the Assad regime, the Syrian FIU remained a member of the Egmont Group. Initially, the Syrian FIU was suspended from participating in the circuit of events and, for instance, was not welcome to participate the annual Egmont Plenary. However, after nine years of suspension, a delegation of the Syrian FIU was again invited to the Egmont Plenary in 2019 in The Hague, the Netherlands (Rasha, 2019).

Furthermore, during the Syrian civil war and despite the known human rights abuses by the Assad government, Syria continued working with the FATF to address and repair its FATF 'non-compliant' rating, stemming from the 2006 mutual evaluation. This means that the international community encouraged and compelled the Syrian government to adopt or strengthen laws that criminalize terrorism financing and money laundering, to expand the list of predicate offences to money laundering and terrorism financing, to enhance customer surveillance of banking clients, and to strengthen customer identification requirements – *while* Assad's atrocities against his own population were ongoing. In 2016, for instance, the Syrian FIU placed 12 requests to Egmont Group FIUs asking for assistance, and received in turn 22 requests via the Egmont Group (Lababidi, 2020, p. 165). The 2018 FATF follow-up evaluation report approvingly notes that prosecutions for terrorism financing in Syria increased from 21 in 2013 to 174 in 2016. This is worrying, especially considering the potential for abuse of these laws for civil society control. The 2018 FATF report on Syria concludes:

> At the level of international cooperation, the amended laws of the Customs Department and the Commission allows exchange of information with foreign counterparts in regards to cross-border monies according to the laws, regulations, agreements and memorandums of understanding that are in place or in accordance with the principle of reciprocity (MENA FATF, 2018, p. 46).

This evaluation of the FATF in 2018 is striking because the civil war continues up to the time of this writing. Even so, the FATF notes that the Syrian FIU was operating in accordance with the "principle of reciprocity". It is not inconceivable that EU governments shared intelligence with Syrian authorities in the context of monitoring 'foreign fighters' wanting to join IS. This example suggests that politics of (dis)trust do not necessarily follow *public* controversies, such as in the case of Uganda and Serbia, but may take place out of public view. Similar to the content of the intelligence that FIUs share being secret and unknown to the subjects they concern, the politics of (dis)trust are and remain opaque unless revealed through public controversy.

43 See https://egmontgroup.org/members-by-region/, consulted August 4, 2022.

Importantly, this politics revolves not only around *whether* to share intelligence with a counterpart FIU – a yes or no – but also around *what types* of intelligence to share. As observed earlier, FIU intelligence encapsulates a range of open and closed information sources, the sharing of which may be more or less sensitive. Open-source information, for example, from the media, are considered less sensitive to share than, for example, credit card information, addresses, and police records.[44] Consider the following reply of a HoFIU to a question about sharing information with 'questionable' countries:

> Of course… when we are speaking about countries that are questionable, both internationally and by the Egmont, then of course we do not exchange data in the same way.… If I give information to [an EU country] I give everything, bank account number, bank, whatever information they want. But if I give information to [a questionable country] I will only say that it is a bank transaction and give an indication of the total amount transferred (HoFIU, August 13, 2019).

The politics of sharing intelligence in the circuit of trust, thus, involves continuous, delicate decision-making processes, which vest considerable responsibility and authority in the hands of an FIU regarding whether, and what types of intelligence, to share with a particular, perhaps 'sketchy', counterpart. The sharing of financial intelligence takes place in a multifaceted political playing field in which individual FIUs autonomously and independently engage in relationships of reciprocity, deliberating on the basis of self-interest and assessments of (un)trustworthiness, and guided by their own assessments of a counterpart's measures of confidentiality and vulnerability to political influence. This vesting of political power and decision-making authority in the hands of these relatively new security actors points to the importance of analyzing how they cooperate transnationally in the absence of public oversight.

6.7 Conclusion

This chapter analyzed how circuits of trust make sensitive financial data and transactions internationally shareable. Given the substantial geographical reach of financial intelligence and expansive nature of monitoring transaction behavior, a better understanding of how citizens' financial data are shared with foreign institutions is important. This chapter has stared from the premise that data do not easily 'flow' across

44 The Egmont Group expects that "[c]ounterparts should be able to provide financial, administrative and law enforcement information and make use of the powers available for domestic analysis in order to obtain the requested information" (Egmont Group 2017, p. 8).

jurisdictions; rather, it takes hard work and practices of building and maintaining trust to render data transnationally mobile. The analysis demonstrates that transnational financial surveillance relies on more than just the infrastructural availability of technologies that enable communication and intelligence sharing (Amicelle & Chaudieu, 2018). These technical platforms and systems also operate through practices and circuits of trust which lie at the core of an FIU's decision to share intelligence.

FIUs were found to work with their own understandings of counterparts' 'trustworthiness' or 'untrustworthiness'. Transnational financial intelligence sharing was demonstrated as taking place in a legal grey zone, and in a context with a high degree of uncertainty and lack of knowledge concerning modi operandi of criminals, as well as obscurity regarding the precise application of legal and data protection frameworks (Mouzakiti, 2020). The qualitative fieldwork demonstrated that personal relations, mutual trust, and informal acquaintance play key roles in processes of financial intelligence sharing, involving political decision-making as well. Circuits of trust are crucial, as these allow practitioners to meet, look each other 'in the eye', and nurture a basis for the sharing and circulation of financial intelligence. The nascent Egmont Group sensitivity shows that awareness of potential misuse of FIU data is increasing, yet little is known about whether and how potential human rights abuses are taken into account when FIUs decide to share financial intelligence transnationally.

Furthermore, this chapter advanced the literature on economic trust practices by introducing the notion of 'circuits of trust,' and drawing out the ways in which trust mediates data sharing. Trust was presented as a 'socio-technical' arrangement (De Wilde, 2020, p. 564), that is unstable and needs to be constructed and maintained in the materiality of practice, through workshops, conferences, and other gatherings at which practitioners meet and engage. This chapter contributes to Zelizer's (2004) notion of "circuits of commerce" by its analysis of the trust practices that permeate seemingly impersonal institutions at the intersection between finance and security. Our analysis of 'circuits of trust' shows how intelligence sharing between FIUs is made possible, but also reveals the fragility of this process, as it is beset with blockages, delays, and legal challenges, that might lead to its breakdown.

Paradoxically, FIUs are often assumed to be, and portrayed as, apolitical organizations, because they are assumed to act independently of the domestic political circumstances in which they operate. According to the Egmont Group (2019, p. 31), "the FIU should be operationally independent and autonomous, meaning that the FIU should have the authority and capacity to carry out its functions freely". However, this autonomy does not exclude politics from financial intelligence sharing, but instead vests considerable decision-making authority and political power in the hands of individual FIUs, because they must decide independently which financial intelligence to share with counterparts on the basis of their trustworthiness. This also entails that in some cases, FIUs might elect not to share certain information with particular counterparts, due to a

perception of their untrustworthiness.

In conclusion, the politics of (dis)trust and data sharing raise questions regarding accountability that need to be subjected to future research. At the time of this writing, it is difficult if not impossible to hold an FIU accountable for its practices. For instance, it remains unknown what happens to shared intelligence after it has been shared, how securely it is stored, and how long a foreign counterpart may own the information. What happens to intelligence that ultimately appears to be insignificant? Perhaps most important, who is accountable when certain FIUs misuse their powers employing shared intelligence? Will an FIU inform national subjects that its sensitive data have been used for these purposes? What independent governmental organizations should monitor the decisions made by FIUs and safeguard against mistakes and illicit practices? The result of the FIU's independence is that the politics of making intelligence shareable remains unchecked and the operations of FIUs are ultimately not subjected to democratic control.

7| Conclusions

7.1 Introduction

This dissertation has examined how Financial Intelligence Units (FIUs) coordinate their operations transnationally and exchange financial intelligence across geographical distance and organizational difference. At the time of this writing, 166 FIUs exchanged financial information via the Egmont Group, their joint platform, in order to trace cross-border transactions indicative of illicit activities, such as money laundering and terrorist financing. However, FIUs are diverse organizations that operate in different economic, institutional, legal, and political environments. Even the ways in which threats, such as terrorist financing, are understood and constructed do not align. FIUs apply different definitions, protocols, procedures, standardizations, and ways of counting and quantifying financial transactions. They construct different versions of financial intelligence and threats, producing different realities in terms of both what these threats are and how they can be combatted. Yet to follow illicit finance across borders, they are bound to join forces and exchange financial intelligence – a massive task, which spans a multitude of jurisdictions, practitioners, legal frameworks, software programs, papers, meeting rooms, relationships of trust, platforms, statistics, regulations, numbers, workshops, and so on.

A growing literature centers on the finance-security nexus (Boy et al., 2017) and the use of commercial financial information for security purposes (Amicelle, 2011; Vlcek, 2012; Wesseling, 2013a, 2018b; Westermeier, 2019). Less is known, however, about the role of the FIU and how this novel security actor handles commercial financial

data (with notable exceptions, such as Amicelle & Chaudieu, 2018; De Goede, 2018; Mouzakiti, 2020). In particular, in the transnational context, the exchange of financial intelligence between FIUs and everyday practices in following illicit financing have remained obscure. This is important to study because financial intelligence includes sensitive personal information, such as names, addresses, bank account numbers, and credit card numbers, potentially from both open and closed sources. These can lead to inferences about "sexual orientation, health status, religious and political beliefs and cultural preferences" (Ferrari, 2020, p. 522). By focusing on the everyday practices of FIUs and their transnational exchange of intelligence, this dissertation aimed to understand how FIUs overcome distance and difference. It set out to understand the dilemmas and challenges faced by practitioners themselves and to identify how different versions of financial intelligence relate, in order to make the exchange of financial intelligence around the globe possible.

Drawing on and speaking to the literatures at the intersection of science and technology studies (STS) and international relations (IR), this research comprised three analytical moves, with which it unpacked the everyday practices of transnational financial intelligence exchange. First, it shifted the focus from cooperation, in which actors seemingly engage in a relational vacuum, to 'co-ordination', a term, including the hyphen, borrowed from Mol (2010, p. 264). The concept of co-ordination helps to bring depth to the analysis, by recognizing the co-existence of different realities of financial intelligence, including the multitude of both human and non-human actors that relate to one another in continuously shifting ways.

Second, drawing on the particular strand of IR research that takes into account the daily practices of transnational processes and the mediation of objects, I emphasized the importance of the materiality of transnational financial intelligence. Following IR scholars in critical security studies (Aradau, 2010; Bellanova, 2017; Bonelli & Ragazzi, 2014; De Goede 2018; Leander, 2021; Salter and Mutlu 2013; Walters, 2014), and what has been termed the 'material turn' (Salter, 2015, 2016), this research considered the (inter) mediation by non-human actors, such as reports, minutes, and software programs, as well statistics, numbering practices, and things as mundane as meeting rooms and schedules. In line with Huysmans' (2011, p. 371) inclusion of seemingly "little security nothings", I argued that trivial things are, in fact, not trivial but form the basis for transnational intelligence sharing and political and geopolitical security operations.

Third, this research applied different vantage points to study transnational processes in the materiality of everyday practices. Drawing, in particular, on the work of Anna Tsing (2005), I adopted different advantageous points of view, to grasp how transnational processes are co-ordinated in practice, where political negotiations and the reconfiguration of power relations take place. Specifically, I adopted as vantage points FIU-the Netherlands (Chapter 3), the EU FIUs Platform (Chapter 4), FIUs' numbering practices (Chapter 5), and circuits of trust (Chapter 6). These different vantage points

made possible the study of transnational processes in practice, from the points of view of intergovernmental organizations, practices, and circuits, though these may potentially be geographically scattered. Using vantage points allowed this research to approach transnational processes, or globalization, not as an abstract thought experiment but as something that occurs in the material reality of practice.

The use of vantage points has both methodological and conceptual advantages. Methodologically, the use of vantage points enables the researcher to 'break free' of a (multi-sited) demarcated research location (Marcus, 1995; Swanborn, 2012), while conducting a flexible, qualitative, and iterative research approach to investigate transnational processes, thus providing rich empirical data with strong internal validity (Bryman, 2008, pp. 37–40). Using vantage points made it possible to focus the research and apply rigorous methodology until data saturation was achieved (Bryman, 2008, p. 412). Conceptually, the use of vantage points enabled me to draw out the moments at which 'friction' rendered the political stakes and reconfigurations of power visible. In actor-network theory (ANT), it is common practice to 'follow' the actor (Latour, 2007). Yet which actor does one follow, in what direction, and for how long? The use of vantage points made it possible in this dissertation to actively search out, recognize, and study those moments at which actors encountered each other and where politics and power became visible and therefore amenable to study.

Taken together, these vantage points enabled me to approach the main research question, of how FIUs work across distance and difference, from a variety of points of view, and provided an in-depth *empirical* understanding of these transnational processes. The main empirical conclusion is summarized as follows: it is the relatively informal nature of international agreements in combination with the autonomy of FIUs that enables FIUs to work across distance and difference and share privacy-sensitive intelligence around the globe. Each of the empirical chapters demonstrated the considerable autonomy that FIUs enjoy to independently decide how financial intelligence is (secretly) produced (Chapter 3), how legal misalignments are solved among the FIUs themselves (Chapter 4), how FIUs generate a shared depoliticized and technocratic vocabulary to coordinate their operations (Chapter 5), and how their autonomy grants them considerable power to independently decide with which counterpart FIUs they share particular intelligence (and which not) (chapter 6). This autonomy to independently maneuver the often informal and non-binding international agreements, such as the FATF recommendations and the principles of the Egmont Group, raises questions of accountability, oversight, and proportionality of FIU operations. These are addressed in this conclusion.

This conclusion revisits the main research findings, bringing together the results of the empirical chapters and drawing out the core contributions of the research. Section 7.2 discusses and connects the empirical, theoretical, and methodological contributions. After this, Section 7.3 reflects on two promising avenues for further academic research. The first concerns how financial intelligence is used and applied further down in the chain

of financial security (De Goede, 2018). A second worthwhile research avenue concerns non-Western FIUs and their growing influence in the transnational co-ordination of financial intelligence. Finally, Section 7.4 turns to the societal relevance of the findings. Throughout the chapters, especially chapters 3 and 6, recurring findings raised the question of what responsibilities and accountabilities FIUs bear, and what safeguards are in place to supervise their operations. In particular, questions are raised concerning the need for safeguards regarding *oversight*, *accountability*, and *proportionality* of FIU activities.

7.2 Empirical, theoretical, and methodological contributions

This section presents the core empirical, theoretical, and methodological contributions of the research. First the empirical contributions are discussed, drawing out the common denominator across the chapters, which is the finding that autonomy in combination with the informal nature of international agreements enables FIUs to work across distance and difference and exchange intelligence. Second, the theoretical contributions are presented, specifically, regarding the broader question of how transnational and global topics can be studied in practice. This discussion has particular relevance in the IR and STS domains, and highlights the conceptual contribution of vantage points and the concepts coined in the separate chapters. Finally the methodological contributions are discussed. These primarily concern how to deploy rigorous methodologies that provide rich empirical detail on geographically scattered processes that span the globe. After highlighting the core contributions, the next section will commence where the last empirical chapter, on trust, ended: with the political and policy-related concerns regarding FIU oversight, accountability, and proportionality.

Empirical contributions

While scholarship on the finance-security nexus has grown (Amicelle, 2017b; Boy, 2017; Boy et al., 2017; Langley, 2017), the operations of FIUs have remained largely opaque and obscure, especially within a transnational context. With a few notable exceptions (Amicelle & Chaudieu, 2018; Mouzakiti, 2020), there is limited academic knowledge of FIUs' everyday practices and their transnational exchange of financial intelligence. This dissertation has aimed to unpack the practices of FIUs and understand the challenges and dilemmas that the practitioners themselves face. In addition to the human actors, it examined the non-human actors, such as reports, emails, statistics, meeting rooms, and the financial transaction reports themselves. Taken together, the empirical chapters answered the main research question by demonstrating that the autonomy of FIUs in combination with the non-binding nature of international agreements makes it possible

for FIUs to coordinate their operations and share financial intelligence in various ways.

Chapter 3 adopted as its vantage point FIU-the Netherlands, zooming in on how this organization (secretly) transforms transaction information into financial intelligence. The chapter draws an analogy with an hourglass. Reporting entities, such as banks and money transmitters, send tens of thousands of unusual transactions to the FIU – which forms the core of the hourglass. The FIU then analyzes this input, producing intelligence which it disseminates to a wide range of security actors, such as the police, secret services, and judiciary. The metaphor of the hourglass emphasizes that the FIU does not merely intermediate the sand – the financial transaction information – but mediates it, by deleting, filtering, and supplementing transaction information, before it becomes accepted and disseminated as financial intelligence. This metaphor, furthermore, indicates the pivotal position of the FIU to independently navigate various intersections, such as that of finance and security, but also that of the private and public sphere and the national and international domain. By analyzing a single FIU's practices in collecting, analyzing, and disseminating financial intelligence, the chapter empirically illustrated the key role the FIU has come to play in the field of financial surveillance, making possible the monitoring of funds and the transaction behavior of citizens.

Chapter 4 adopted the EU FIUs Platform as its vantage point. This is an expert group of the European Commission, including at the time of this writing 30 EU FIU members which gathered periodically in Brussels to discuss practical, technological, and technocratic issues concerning intelligence sharing. The chapter meticulously analyzed the minutes of meetings of this platform, in particular, the agenda item "obstacles to sharing/dissemination of information", which centered on the phrase "for intelligence purposes only" (European Commission, 2015, p. 7). The phrase, which was attached to financial intelligence shared between the FIUs and served as a type of safeguard against abuse, became a key topic, causing heated debates among the FIUs. A close examination of this debate unearthed core policy issues and political stakes concerning transnational financial intelligence sharing. Seventeen FIUs were not prepared to share their intelligence with foreign counterparts if the intelligence could be used as evidence in a courtroom proceedings. The clause was therefore adjusted to offer two options, specifying whether or not the intelligence may be used as legal evidence, with the intelligence still shared in either case. This chapter yielded insights into how geographically dispersed FIUs manage to produce and navigate common understandings of data sharing. It demonstrated that FIUs, among themselves, have the power to independently decide how legal issues, such as the privacy of intelligence, should be handled and solved.

Chapter 5 adopted numbering practices as its vantage point. From this point of view, it became possible to grasp how FIUs co-ordinate their operations through the statistics and numbering practices they deploy to work across seemingly incommensurable differences. Because FIUs apply a variety of different definitions of

terrorism and terrorist financing, the way in which these concepts are constructed and known to FIUs constitutes different versions, different realities of what these security threats entail. The FIUs' different definitions, ways of measuring, protocols, and procedures yield differently generated numbers and statistics. However, this spectrum of statistics and numbering practices does not prevent the FIUs from bridging distance and difference, but instead makes such bridging possible by providing a shared technical and often technocratic vocabulary through which FIUs can engage. Through statistics and numbering practices, FIUs relate and encounter one another, steering through tensions, conflicts, (mis)alignments, (mis)understandings, negotiations, and collaborations, without touching on the question of what terrorism actually entails.

The final empirical chapter, Chapter 6, adopted the vantage point of circuits of trust, focusing on the politics of coordinating financial intelligence and sharing sensitive financial intelligence. This chapter, particularly, provided a view on the autonomy of FIUs to independently decide with which counterparts to share particular types of information (and which not). The circuit of conferences, workshops, and webinars provides FIUs opportunities to build and maintain informal relationships of trust, based on which financial intelligence can be shared. Given that 166 FIUs have committed to share financial intelligence through the Egmont Group, the intelligence travels and translates to a diversity of political, economic, cultural, and legal contexts. FIUs, therefore, need to trust that the counterparts with whom they share intelligence will handle their data with confidentiality and care. This is imperative, because there have been cases in which FIUs have not operated in an autonomous and independent fashion, but instead been used by governments to suppress critical civil society actors. As a result, the sharing of sensitive financial intelligence relies on implicit notions of trustworthiness/untrustworthiness of counterpart FIUs. The chapter concluded that the delicate politics of (dis)trust raises important concerns about the authority of FIUs and their power to decide who they can share information with, touching on questions of responsibility and accountability in FIU operations.

Taken together, the empirical chapters provide a good understanding of how FIUs manage to work across distance and difference, and on the basis of their autonomy, to operate independently within a context of loosely defined, informal, and non-binding regulations. As Chapter 6 in particular demonstrates, FIUs operate in a legal grey zone that is governed by 'recommendations', 'principles', 'guidelines', and mutual evaluations, instead of, for instance, by rules, laws, and treaties. Chapters 3 and 5 demonstrate how autonomous FIUs are in regard to their internal processes, demonstrating respectively, that they transform transaction information into financial intelligence in a cloud of secrecy and generate particular constructs of what security threats such as terrorist financing are. Chapters 4 and 6 demonstrate how FIUs encounter one another through international organizations, in which they operate as a collective of independent actors that determine, respectively, how legal regulations on privacy

should be handled and on what basis and reasonings intelligence should or should not be shared. Finally, chapters 3 and 6 address the societal consequences of the autonomy of FIUs to operate relatively independently. In particular, in a transnational context this raises urgent questions concerning accountability and proportionality, because the Egmont Group includes members with questionable reputations regarding important concerns, such as privacy and human rights, including Egypt, Belarus, Russia and Saudi Arabia. These societal consequences will be unpacked further in Section 7.3.

Theoretical contributions

The question of how to study transnational or global topics in daily practice has received consideration from a diversity of disciplines, such as STS (Bowker & Star, 2000; Latour, 2007; Law, 1986, 2002), IR (Barry, 2013; Bueger & Gadinger, 2014; Salter, 2015), and what can be roughly understood as the anthropology of globalization (Appadurai, 1996; Tsing, 2005). Regarding financial intelligence, for instance, De Goede (cited in Salter et al., 2019, p. 31) asks, "How can observations of the 'small' of quotidian transactions analysis practices at banks or data companies tell us something about the 'big' of contemporary geopolitics?" I have proposed to adopt certain vantage points that provide views on the coordination of transnational processes in practice. This research has demonstrated that using different vantage points makes it possible to study geographically scattered processes of grand scope, such as financial intelligence, in the reality of material practice. Furthermore, three of the empirical chapters provided conceptual tools to further assist in this effort.

Chapter 4 applied a 'flat ontology' in order to understand how the EU FIUs Platform generates shared understandings of transnational financial intelligence. It argued that to study "formations of scope" such as the transnational or global (Bueger & Gadinger, 2014, p. 65), we need to turn to how scales are brought into being and maintained in the materiality of practice (Latour, 2007, pp. 171–172). The chapter argued that practices do not constitute an imaginative social construct or linguistic speech act, but a material reality that is constructed in various places, documents, (digital) environments, and suspicious transaction reports. Drawing on work at the intersection of actor-network theory and IR, the chapter proposed two concepts that assist in the study of formations of scope in practice. The first concept concerns the 'interpretive flexibility' of objects. Inspired by the notion of 'boundary objects' by Star and Griesemer (1989), I investigated how the clause 'for intelligence purposes' allowed practitioners to generate shared understandings only because the clause can adapt to local needs, while simultaneously being "robust enough to maintain a common identity across sites" (ibid., p. 393). Building on this concept, second, the chapter developed the notion of 'flexible scalability' to acknowledge the multifarious nature of scale-making processes. I argued that practitioners assign and navigate different scales themselves, in practice. It therefore becomes redundant to assign scales as a researcher, because the

production of formations of scope is firmly situated in practice and can therefore be empirically studied via 'small' observations.

Based on the analysis of numbering practices in the global sharing of financial intelligence, Chapter 5 advanced STS literature on the geographical circulation of knowledge via the harmonization or standardization of practices. This chapter speaks to classic STS scholarship on standardization (Porter, 1996), routinization of practices (Desrosières, 1998), and the 'universalization' of metrology standards (Latour, 2007, p. 229), as well as recent work on data (Leonelli, 2016) and the maintenance of infrastructures (Denis & Pontille, 2019). Drawing in tandem on the work of Mol on multiplicity (2002) and that of Tsing on 'friction' (2005), the chapter demonstrated that knowledge of terrorist financing circulates because of its multiplicity and the lack of harmonization or standardization of practices. It found that knowledge of terrorist financing can be made to travel through the disparate practices, through collision, conflict, or collaboration, instead of alignment or calibration. From this angle, statistics and numbering practices to encapsulate terrorist financing are a means of coordination that provides infrastructural substance by generating a shared technical, depoliticized, and often technocratic vocabulary and a sense of urgency and legitimacy for FIUs to share privacy-sensitive financial intelligence around the globe.

Studying the sharing of intelligence in practice, furthermore, Chapter 6 turned to circuits of trust. The chapter uncovered the 'legal grey zone' in which FIUs operate, marked by a high uncertainty and lack of knowledge on the workings of financial crime, as well as by unclear and often ambiguous implementations of legal and data protection legislation (Mouzakiti, 2020). The chapter takes inspiration from the work of Zelizer (2006, 2004) and her notion of 'circuits of commerce', and proposes to study what are termed 'circuits of trust' in order understand the politics of transnational intelligence sharing. Trust is understood as a "socio-technical arrangement" (De Wilde, 2020, p. 564) in which practical work is required in order to make intelligence sharable. Drawing on participant observation of the networks at the events, conferences, workshops, and seminars where trust is generated and interpersonal connections are fostered, the chapter examined three practices: the use of trust circuits to navigate the 'legal grey zone' in which FIU data are shared; the way trust circuits make intelligence sharing possible (or not); and how the implicit notions of trustworthiness and untrustworthiness lead to inclusion/exclusion. In doing so, the chapter illustrated that co-ordination of practices requires considerable autonomy of FIUs, to independently decide what types of information to share with what counterparts. This raises questions of institutional safeguards, such as accountability and oversight, to which the next section turns.

These three chapters offer conceptual tools that make it possible to address transnational or global processes by studying practice. To recapitulate Tsing (2005, p. 58), "many ethnographers find ourselves with data about how a few people somewhere react, resist, translate, consume, and from here it is an easy step to invoke distinctions between

local reactions and global forces". Though the current research cannot be considered an ethnography, because it does not include extensive and prolonged fieldwork within a particular situated context, it does provide the conceptual tools to study transnational processes in practice, not limited to the topic of financial intelligence. Use of 'vantage points' and concepts such as 'interpretive flexibility', 'flexible scalability', and 'circuits of trust' contributes to a broader debate at the intersection of IR and STS. As Salter (2015, p. xvi) writes, "For the discipline of international relations,… [the] new materialist sensibility toward open inquiry without pregiven scales of analysis poses a powerful and immediate intellectual challenge". The conceptual contributions of this dissertation hopefully make some advances to addressing this challenge.

Methodological contributions

This dissertation has demonstrated that the use of different vantage points enables the researcher to gather rich empirical data on grand-scale transnational processes. Quantitative research designs are often associated with strong generalizability, yet uncertain internal validity, while qualitative research designs are considered to have strong internal validity, yet poor generalizability (Bryman, 2008, pp. 37–40). For this reason, the latter is often considered to be suitable primarily to study a demarcated field worksite or clearly defined case study (Swanborn, 2012). By studying moments at which transnational processes are co-ordinated in practice, the methodological design of the current research demonstrates that qualitative methods can also be valuable to study and understand geographically scattered processes, such as financial intelligence exchange. Instead of turning to concepts such as the 'international' or 'global' to study transnational processes, I employed qualitative methods to gather in-depth empirical data on practices that are connected around the globe. Following STS and ANT, I not only studied human aspirations, but also included (material) actors that to some inevitable extent mediate or intermediate the state of affairs (Callon, 1984; Laet & Mol, 2000; Latour, 1999; Star, 1990). This research thus included the materiality of transnational processes, such as the meetings of the EU FIUs Platform (including minutes and agendas), the debates on numbering (including documents), and the circuits through which practitioners encounter one another at conferences, workshops, and other digital and physical gatherings.

Adopting vantage points had two methodological advantages. First, it assisted in choosing how to iteratively commence the research. This is especially challenging when studying topics of transnational or global nature, with a multitude of possible starting points and actors to follow. In ANT, it is often proposed to 'follow' the actors (Latour, 2007). For instance, De Goede (2018) has found that following a single financial transaction can yield valuable insights regarding the chain of financial intelligence through which a transaction travels and is translated from banks, to FIUs, to perhaps, law enforcement agencies. Furthermore, as Amicelle (2017a) has demonstrated, ethnographic findings within a bank or FIU can generate findings reflecting broader

features of financial intelligence. What vantage points bring, in terms of methodology, is that they assist in the choice of which actors to pursue, and guide the identification of favorable points of view that enable the researcher to study moments at which political stakes and the reconfiguration of power relations become visible. Using the grounded theory approach (Glaser & Holton, 2004; Glaser & Strauss, 1967), I switched back and forth between empirics and theory, thereby gradually sharpening the research approach and questions, and distilling the vantage points that appeared most interesting, informative, and academically valuable to study.

The second advantage of applying vantage points was to enable the research to deviate from a linear trajectory, and instead to flexibly explore parallel research avenues simultaneously until data saturation was reached. This meant that the data gathered could find purpose in several ways at different points in the research process. I applied different strategies and methods, such as 'snowball sampling', to move from one respondent to another (Bryman, 2008, pp. 184–185), the 'encircling of secrecy' approach, to bring the larger picture into focus by studying "the mundane lifeworlds of security practices and practitioners" (Bosma et al., 2019, p. 14), and engaging in participant observation (Spradley, 1980). I applied an inductive and iterative research strategy to pursue several promising research paths in parallel, alongside the aforementioned grounded theory approach (Glaser & Strauss, 1967), to sharpen my research questions and select the best vantage points. The research as a whole is based on 29 interviews with 37 practitioners; participant observation at conferences, workshops, and seminars; and extensive document analysis including meeting minutes, annual reports, regulations, and policy reports (see Table 2.1).

7.3 Suggestions for future research

This research sought to unpack and understand the everyday practices of FIUs and their transnational exchange of financial intelligence. It asked how do FIUs co-ordinate their operations and work across distance and difference. Each empirical chapter used a different vantage point to shed a particular light on the main research question. Inevitably, however, the research occasionally faced difficult choices concerning what research paths to pursue, and which ones to let pass. This final section presents two avenues of research that appear particularly fruitful and which I would have pursued if practical challenges – mainly time and money – had allowed. The first is to some extent a continuation of the final point of the previous section on proportionality: to answer the question of what exactly the proceeds of financial intelligence are. The second research avenue concerns an element of the transnational FIU landscape that could receive very little consideration in this dissertation: the increasingly prominent role of non-Western FIUs.

On the proceeds of financial intelligence

This research focused on one part of the 'chain of security' (De Goede, 2018), whereby financial transactions travel and are translated from commercial actors, such as banks, to the FIU, to law enforcement, to eventually – possibly – be used as evidence in a court of law. FIUs are an important link in this chain, located in between the private sector and the public sector, receiving financial information from banks, and disseminating financial intelligence to public security actors. However, how this intelligence is eventually utilized further down the chain, often remains unspecified and unclear. Anwar (2020, 2021) has offered in-depth understanding of court cases concerning terrorist financing in the Netherlands (see also Anwar & De Goede, 2021). Yet, these cases do not arrive in a courtroom based only on intelligence from an FIU; rather, regular law enforcement investigations can play the key role. Furthermore, regarding money laundering in the Netherlands, an employee of the Public Prosecution Service estimated that in 2020 only a dozen court cases derived from financial intelligence from the FIU.[45] Except for anecdotal information from FIUs,[46] there is, to my knowledge, no quantitative information available that offers an impression on how financial intelligence is deployed by actors further down the security chain.

It is important to realize that intelligence does not have to result in a court case or conviction to be utilized for security purposes. It can provide a small but potentially significant piece of an intelligence puzzle, advancing an investigation without this being publicly known. One investigative journalist calculated that financial intelligence from FIU-the Netherlands led to only a 0.083% change in conviction rate, leading to the conclusion that countering money laundering is "hopelessly ineffective" (Janssen, 2022). However, this conclusion refers only to convictions. As observed in this dissertation, particularly in Chapter 3, the intelligence is often made available to a wide range of investigative and prosecution services, such as the police, special agencies, intelligence services, security services, and the Public Prosecution Service. Furthermore, the FIU cooperates directly with a variety of partners. For instance, in the Netherlands it developed a healthcare fraud monitor with the Social Affairs and Employment Inspectorate (ISCW) (FIU-Nederland, 2021, p. 27). As such, FIUs can be part of a spectrum of public-private partnerships. Although financial intelligence flows to a plethora of actors, down the line it becomes unclear how exactly the intelligence is deployed.

The inability to assess the proceeds warrants further academic research, inquiring not only into potential court cases but also focusing on the many ways in which intelligence is being deployed. Whether trivial or substantial, it is important to come to know how intelligence might (or might not) contribute to, crudely put, a safer world. A clear idea of the potential proceeds of FIU activities is key in order to

45 See https://www.trouw.nl/economie/tienduizenden-witwasmeldingen-amper-strafzaken-soms-lijkt-het-of-het-hele-meldsysteem-voor-niets-is~b03c7f64/, consulted on June 8, 2021.

46 See, e.g., https://www.fiu-nederland.nl/nl/wetgeving/casuistiek, consulted on April 1, 2022.

adequately deliberate on the question of whether financial intelligence is proportional, given its privacy challenges and unintended consequences. In-depth knowledge of the security gains or proceeds is also crucial to formulate informed political positions on FIU activities and organization, and as well as to provide a basis for policy.

Non-Western FIUs and the global expansion of the FATF

This research focused primarily on Western FIUs. The reason is twofold. First, the research applied a European scope corresponding to the broader FOLLOW research project of which it was part, supported by a European Research Council (ERC) grant. Furthermore, the research was based in the Netherlands and the network with practitioners was initially developed locally, with connections to FIU-the Netherlands and other national practitioners. From here the research expanded to include the EU (specifically, the EU FIUs Platform) and eventually the Egmont Group, the global platform for intelligence exchange between FIUs. The second and connected reason why primarily Western FIUs were within the scope of the research is the fact that the FIU landscape was and still is dominated by FIUs from Western countries, in particular from Europe, the US, Canada, and Oceania. While the FATF and the Egmont Group currently include FIUs and countries around the globe, this is a relatively recent occurrence. Initially, both the FATF and the Egmont Group comprised primarily Western countries and FIUs. Even at the time of this writing, while non-Western members are part of the organizations, it is the Western members that hold sway in these intergovernmental institutions. In the case of the FATF, this has changed to some extent in recent years, as all of the BRICK countries have joined and increasingly occupy important positions (e.g., China delivered the president of the FATF in 2019–2020). However, in the Egmont Group, the most prominent positions are still held by Western FIUs. For instance, FIU-the Netherlands held the presidency at the time of this writing.

However, the geopolitical balance is shifting, as I observed during the fieldwork. The Egmont Group is actively including and training non-Western FIUs via its learning center, ECOFEL, and I encountered representatives of non-Western countries actively seeking to acquire a place at the table. Further study of the emerging and novel role of non-Western FIUs in the transnational co-ordination of financial intelligence is therefore timely and relevant. For instance, how do countries that until recently did not have an active FIU, establish this organization – bring such an organization into being – and decide on its mandate, on which basis it may act transnationally? How does a recently established FIU become part of the global circuit of trust and engage in the politics of (dis) trust that enables an FIU to access foreign intelligence (see Chapter 6)? Such questions connect to current debates on postcolonialism, for instance, on how infrastructures that were established in the past echo into the present (Bellanova & De Goede, 2022; De Goede, 2021). It would be interesting to investigate how the infrastructures of the FATF and the Egmont Group, which were established relatively recently, though during the

hegemony of Western countries, might be challenged, negotiated, or even altered in the years to come.

7.4 Societal consequences

Building on the methodological, empirical, and theoretical contributions, several key societally relevant research findings emerge from this research. A recurring theme throughout this dissertation, and particularly, in chapters 3 and 6, concerns the societal consequences of the independence and autonomy of FIUs and the lack of institutional safeguards. By granting FIUs such institutional autonomy, considerable political power to independently make important and decisive decisions is transferred to and vested in FIUs. Given that the FIU is a relatively new organization, and financial intelligence in a broad sense is a new phenomenon that has only become possible with the digitalization of payment transactions and spending behavior, the political and policy-based concerns remain to be thoroughly addressed. In both academic and public discourse, financial intelligence and its implications has not received the contemplation nor scrutiny that it pragmatically requires and ethically deserves (notable exceptions are Dehouck & De Goede, 2021; Mitsilegas & Vavoula, 2016). As Mitsilegas and Vavoula (2016) argue, the translation of global standards, as formulated in the FATF recommendations, into regional and national legislation, can have far-reaching consequences for national rights. "The more these [FATF] standards develop in this manner", these authors note, "the more likely it is for the EU legislator to face constitutional and fundamental rights objections" (ibid., p. 292).

Furthermore, in relation to the fight against terrorism financing and the public-private initiatives involved, Dehouck and De Goede (2021) propose that there are pressing legal and ethical stakes, such as democratic legitimacy, privacy and proportionality, rights of individuals, and accountability. According to these authors, addressing these concerns does not necessarily require solutions or recommendations; rather, they can be addressed by posing *questions* that can serve as valuable tools for further societal debate (ibid., p. 10). To advance that process, this section draws together empirical findings from this research that may help in addressing important concerns at the intersection of politics and policy. Particularly, these concern the need for safeguards regarding *oversight*, *accountability*, and *proportionality*.

Oversight

Because international recommendations and guidelines prescribe that FIUs must be autonomous and independent (Egmont Group, 2019; FATF, 2022, p. 104), their political decision-making processes, operational details, and bilateral and multilateral collaborations often remain opaque and inaccessible to outside judgement. This is

surprising because of the sensitivity of the intelligence that FIUs collect without the consent or knowledge of the – not officially charged – 'suspect' whose information is stored in FIU databases (see Chapter 3). To come to know FIU operations in a procedural sense, this research applied strategies such as "encircling the secrecy" (Bosma et al., 2019, p. 3), yet it remains unclear whether and to what extent actual FIU operations are subjected to external oversight and control. As Mouzakiti (2020) points out, the EU directives on police data and data protections are to some extent at odds but also differently applied by FIUs. Furthermore, the issue of oversight is not so much a question of safely protecting or storing data or following legal and technocratic regulations, but of whether there is an internal or external institutional safeguard that is equipped to independently monitor and control the daily operations of an FIU and how it disseminates data both nationally and transnationally (see Chapter 4).

Nationally, the question of oversight is important because financial information collection relies to a considerable extent on automated security 'decisions', in which transactions are flagged as suspicious based, for instance, on 'objective' thresholds or involvement of high-risk countries (see Chapter 3 and 5). As an example, because of the unbalanced ratio in the Netherlands between the millions of reports received and the limited human and financial capacity to investigate these, many transactions are classified as suspicious without human interference, or the involvement of a public prosecutor, investigating judge, or any other human intervention. This is remarkable given the considerable privacy breach once a transaction is declared suspicious and copied into the suspicious transactions database, which is accessible to almost the entire Dutch police force via the software BlueView. Moreover, the information remains in that database for ten years (see Chapter 3). The highly automated system raises questions about who supervises the decisions and authority of the FIU to declare transactions suspicious, and whether this authority requires internal or external independent oversight. What independent control and monitoring is being conducted on the daily operations of the FIU? How could the authority of the FIU to automatically (or manually) categorize transactions as suspicious be subjected to external institutional control by, for instance, a ministry, judiciary, or within the police?

At the transnational level, the question of oversight amplifies in importance because FIUs are committed to exchange financial intelligence with counterparts in the Egmont Group – which had 166 members at the time of this writing (see Chapter 6). What national or transnational organization monitors whether the financial intelligence that is shared stays within the FIU with which it was exchanged, and does not travel beyond to other security actors to at some point become impossible to trace? Who ensures that the shared intelligence is not being used for illicit purposes, such as the suppression of civil society actors? Because the Egmont Group includes members with questionable reputations in terms of human rights and adherence to privacy standards, it is concerning that EU FIUs can share intelligence with these types of counterparts

without supervision or possible interference by a third party that monitors the necessity and justness of the exchange. Especially when considering the opaque oversight at the national level and the fact that intelligence is often automatically categorized as suspicious, the ability to share this intelligence unchecked with autocratic regimes can have unforeseen consequences (see Chapter 6). How could transnational exchange of financial intelligence be supervised, in order to guarantee that intelligence does not disseminate further to third parties or be used for illegitimate purposes? What safeguards are in place when financial intelligence is shared with questionable, possible autocratic or dictatorial regimes?

Because it is unclear what intelligence is shared transnationally, as this remains behind closed doors – which is understandable from a security perspective – the transnational exchange itself remains obscure, and it remains unclear to what institutional oversight the operations of FIUs are subjected (see chapters 4 and 6). Debates on the transnational exchange of intelligence are often technological and technocratic in nature, such as whether 'interoperable' software systems can provide initial anonymity of data (Kroon, 2013). However, the legal grey zone in which FIUs operate raises questions beyond technological, technocratic, and bureaucratic challenges (see Chapter 5 and 6). The key issues at stake are political in nature. An important question, for instance, is whether intelligence *should* be shared globally on the basis of loosely defined recommendations, guidelines, principles, practices, and circuits of trust. What rules, laws, or treaties – in addition to the existing recommendations, guidelines, and principles – could stipulate the ways in which FIUs share their intelligence? What oversight and safeguards should be in place to monitor whether these are adhered to? Indeed, an answer to these questions seems extremely challenging, given the diversity of FIUs. Yet, if a solution is improbable, then the political question should be put on the table of whether it is desirable and just to exchange intelligence transnationally.

Accountability

The opaque nature of national and transnational oversight is particularly important with respect to the question of accountability. As Dehouck and De Goede (2021, p. 27) write in relation to public-private partnerships in the fight against terrorist financing, "oversight and accountability can help address some of the potential harms of profiling, mistakes and misuse". With respect to specifically the FIU, the issue of accountability is pertinent because it operates at the intersection of private and public actors as well as of the national and international domain. For instance, FIU-the Netherlands is an independent and hybrid organization that is institutionally connected to two ministries, but simultaneously it is operationally embedded within law enforcement.[47] This raises

47 FIU-the Netherlands is a so-called 'independent government branch' (zelfstandige bestuursorgaan). This means that the FIU has special rights – in the case of the FIU, to handle sensitive financial intelligence – and is not subject to the direct supervision of a ministry. The minister does have some responsibilities

two important concerns: to whom does the FIU answer and who is accountable when someone makes a mistake and when, unintendedly, people come to harm as a result?

The first question, on responsibility, is increasingly important in light of FIUs' active pursuit of new ways to disseminate their intelligence (see, e.g., Amicelle, 2020). In the Netherlands, as observed in Chapter 3, the FIU proactively searches for new ways to use financial intelligence for security purposes, such as new 'confiscation projects' to seize luxury items from criminals in cooperation with other intelligence departments and projects to trace fraud in healthcare, such as development of a 'healthcare fraud monitor' (see, respectively, RIEC-LIEC, 2020, p. 22; FIU-Nederland, 2021, p. 27). In this multilayered field in which financial intelligence is disseminated and circulates without clear oversight or control and is utilized in experimental ways, it becomes challenging to understand who is responsible if something goes wrong. The fluidity of intelligence circulation and its novel security applications decentralizes responsibility and accountability (Bauman & Lyon, 2013). What organization or person is responsible and accountable for the ways financial intelligence is used further down the security chain, for example, by police, secret services, and prosecutors? Should the FIU be held responsible for the many ways its intelligence might be used by security actors, nationally and internationally?

The question of who is responsible and therefore accountable is especially important regarding unforeseen consequences of intelligence use. For instance, a mistake may be made or someone might have been disproportionately harmed because of its use (we return to this below in the discussion of proportionality). Because it is unclear who is responsible, "'It's not my department' would be the quintessential bureaucratic response to queries about the rightness of an official assessment or judgement" (Lyon 2013, cited in Bauman & Lyon, 2013, p. 13). In particular, because the person whose information is stored in databases is unaware that private information might circulate to a wealth of security actors, both national and international, there is no recourse to determine what security decisions may be made on the basis of financial intelligence or, in effect, to hold an organization or person accountable in case of a mistake. When should citizens be informed about storage of their financial data? Indeed, sharing such information would pose substantial challenges in a security sense, because potential criminals would also be informed. However, given that financial surveillance is often not targeted, but involves the mass collection of data, the question of whether citizens should have the possibility to – either automatically or upon request – enquire as to whether private information is stored and possibly circulated to national security actors and international FIUs, warrants more political and policy-related scrutiny.

7

(see Section 3.6). Also, see https://www.rijksoverheid.nl/onderwerpen/rijksoverheid/zelfstandige-bestuursorganen, consulted January 28, 2022.

Proportionality

The notion of proportionality is often related to law and human rights. According to Sieckmann (2018, p. 3), "proportionality is the standard that guides the balancing of human or fundamental rights in law, requiring that the interference with rights must be justified by reasons that keep a reasonable relation with the intensity of the interference". In this regard, my interest in proportionality is not in a legal or human rights sense *per se*, but rather in the normative and political sense concerning justification and the "intensity of interference" (ibid.). Are the security proceeds and benefits proportional to the individual and societal interference and costs? As observed in chapters 3 and 6, the security proceeds of financial intelligence are difficult to estimate, both within any national jurisdiction where – to my knowledge – only anecdotal and no quantitative data are available, but especially transnationally where the exchange and use of financial intelligence remains obscure. Yet, for the question of proportionality, we can take as a starting point the fact that the proceeds of financial intelligence sharing are unclear, within the security sector, in public debate, and in the academic literature. Given that the security proceeds are unclear and at best modest (see particularly Section 3.6), to what extent is financial intelligence (and its impacts) proportional? Two aspects are especially important here: (1) the scope and scale of data collection and its consequences for privacy and (2) the unintended consequences and side-effects of financial intelligence.

The first aspect raises the question of the extent to which it is reasonable that millions of transactions and other types of information are collected and stored without the knowledge of the population being surveilled. Leaving aside the technological and technocratic questions of whether the data are safely stored and the practitioners thoroughly vetted, it is a political question whether it is acceptable in a societal sense to conduct large-scale financial surveillance with considerable privacy consequences. For instance, what assumptions and normative deliberations – either from a security or a safeguarding perspective – underlie the decision in the Netherlands to store unusual transactions in a database for a period of five years? Perhaps more important is the case of *suspicious* transactions, because the privacy breach here is more substantial. What assumptions and normative deliberations underlie the decision to store intelligence on transactions deemed suspicious for a period of ten years, while the subjects of the information stored and circulated are not informed or officially named as suspects? In the case of the Netherlands, there is furthermore the question of why suspicious dossiers that have been investigated and not proven to involve any type of crime (about a third of the dossiers), are still retained in the database of suspicious transactions, which is widely made available to law enforcement via the software BlueView (see Chapter 3). When should transaction information and intelligence, after investigation proves it does not involve illicit activities, be deleted from both databases? To what extent is data retention proportional, given the privacy breach in both databases and the unclear security proceeds further down the chain? To what extent is the importance of privacy

and transparency proportional to that of security and secrecy?

The second point that weighs in on the balance of proportionality, in addition to the privacy breach, concerns unintended consequences and side-effects. Examples of these are the economic impact, de-risking, and de-banking. Economic impact refers primarily to the financial and human costs that accrue to banks, and are increasingly passed on to banking consumers. Are these proportional to the security efforts and benefits further down the chain? According to recent estimations, large banks in the Netherlands employ some 12,000 employees for client and transaction monitoring, while FIU-the Netherlands had only 76 employees in 2020. Furthermore, whereas banks spend thousands of millions to execute their financial monitoring tasks, FIU-the Netherlands has only a fraction of that budget, €9 million in 2020 (FIU-Nederland, 2021). The extreme divergence between the human and financial capacity of banks and that of the FIU raises the question of whether banks' massive monitoring of transitions and consumers is proportional, given the FIU's moderate capacity. Furthermore, the substantial requirements that banks must comply with lead increasingly to side-effects such as de-banking, which is the refusal to give a potential customer a bank account, due to a purported risk they might pose (Durner & Shetret, 2015). In order to 'de-risk' their client database, de-banking of customers has taken flight, particularly in 'risky' domains such as NGOs working in conflict areas (ibid.). How can unintended consequences and side-effects such as de-banking and financial exclusion be mitigated?

Table 7.1 summarizes the questions raised concerning oversight, accountability, and proportionality at the intersection of policy and politics. They can – hopefully – serve as food for thought for future debate, of interest not only to academics, but to politicians, policymakers, and practitioners as well.

TABLE 7.1: Questions for policymakers and political and public debate. Source: Author.

Institutional oversight	*National oversight* • What independent control and monitoring is being conducted on the daily operations of the FIU? • How could the authority of the FIU to automatically or manually categorize transactions as suspicious be subjected to external institutional control by, for instance, a ministry, the judiciary, or within the police? *Transnational oversight* • How could transnational exchange of financial intelligence be supervised, in order to guarantee that intelligence does not disseminate further to third parties or be used for illegitimate purposes? • What safeguards are in place when financial intelligence is shared with questionable, possibly autocratic or dictatorial regimes? • What rules, laws, and treaties – in addition to the existing recommendations, guidelines, and principles – could stipulate the ways in which FIUs share their intelligence?
Accountability	• To whom does the FIU answer? • Who is accountable when someone makes a mistake and when, unintendedly, someone is harmed as a result? • What organization or person should be responsible and accountable for the ways in which financial intelligence are being used further down the security chain, for example, by the police, secret services, prosecutors, and foreign FIUs? • Should the FIU be held responsible for the ways in which its intelligence might be used by security actors nationally and internationally? • When should citizens be informed about storage of their financial data?
Proportionality	• Are the security proceeds or benefits of FIU activities proportional to the individual and societal interference and (unintended) costs? • When should transaction information and intelligence that after investigation proves not to involve illicit activities, be deleted from all databases in which it is stored? • To what extent is data retention proportional given the privacy breach and unclear security proceeds further down the chain?

Bibliography

Abrahamsen, R., & Leander, A. (2016). *Routledge Handbook of Private Security Studies*. Routledge.

Acuto, M. (2015). Garbage. In M. B. Salter (Ed.), *Making Things International 1: Circuits and Motion*, 266-281. University of Minnesota Press.

Adler, E., & Pouliot, V. (2011). International Practices. *International Theory*, 3(1), 1–36.

AFM, [Autoriteit Financiële Markten]. (2020). Leidraad Wwft en Sanctiewet: Toelichting op de Wet ter Voorkoming van Witwassen en Financieren van Terrorisme en de Sanctiewet 1977.

AG Connect. (2008). Politie is zeer tevreden over BlueView. *AG Connect*. https://www.agconnect.nl/artikel/politie-is-zeer-tevreden-over-blueview, consulted on 17 May 2021.

Akse, T. (2019). *Na de poortwachters: 25 jaar meldingen ongebruikelijke transacties*. FIU-Nederland.

Amicelle, A. (2011). Towards a "New" Political Anatomy of Financial Surveillance. *Security Dialogue*, 42(2), 161–178.

Amicelle, A. (2017a). Policing Through Misunderstanding: Insights from the Configuration of Financial Policing. *Crime, Law and Social Change*, 69(2), 207–226.

Amicelle, A. (2017b). When Finance Met Security: Back to the War on Drugs and the Problem of Dirty Money. *Finance and Society*, 3(2), 106–123.

Amicelle, A. (2020). Right of Entry: The Struggle over Recognition in the World of Intelligence. *Political Anthropological Research on International Social Sciences (PARISS)*, 1(2), 243-272.

Amicelle, A., & Chaudieu, K. (2018). In Search of Transnational Financial Intelligence: Questioning Cooperation Between FIUs. In C. King, C. Walker, & J. Gurule (Eds.), *The Palgrave Handbook of Criminal and Terrorism Financing Law*, 649-675. Palgrave Macmillan: Cham.

Amicelle, A., & Favarel-Garrigues, G. (2012). FINANCIAL SURVEILLANCE: Who Cares? *Journal of Cultural Economy*, 5(1), 105–124.

Amicelle, A., & Jacobsen, E. (2016). The Cross-Colonization of Finance and Security Through Lists: Banking Policing in the UK and India. *Environment & Planning D: Society and Space*, *34*(1), 89–106.

Amoore, L. (2013). *The Politics of Possibility*. Duke University Press.

Amoore, L., & De Goede, M. (2008a). *Risk and the War on Terror*. Routledge.

Amoore, L., & De Goede, M. (2008b). Transactions after 9/11: The Banal Face of the Preemptive Strike. *Transactions of the Institute of British Geographers*, 33(2), 173–185.

Anwar, T. (2020). Unfolding the Past, Proving the Present: Social Media Evidence in Terrorism Finance Court Cases. *International Political Sociology*, 14(4), 382-398.

Anwar, T. (2021). Time Will Tell: Defining Violence in Terrorism Court Cases. *Security Dialogue*, 53(2), 1–17.

Anwar, T., & De Goede, M. (2021). From Contestation to Conviction: Terrorism Expertise before the Courts. *Journal of Law and Society*, 48(2), 137–157.

Appadurai, A. (1996). *Modernity at Large: Cultural Dimensions of Globalization*. University of Minnesota Press.

Aradau, C. (2010). Security That Matters: Critical Infrastructure and Objects of Protection. *Security Dialogue*, 41(5), 491–514.

Aradau, C. (2017). Assembling (Non)knowledge: Security, Law and Surveillance in a Digital World. *International Political Sociology,* 11(4), 327–342.

Aradau, C., & Huysmans, J. (2014). Critical Methods in International Relations: The Politics of Techniques, Devices and Acts. *European Journal of International Relations*, 20(3), 596–619.

Armstrong, G., & Norris, C. (1999). *The Maximum Surveillance Society: The Rise of CCTV*. Berg Publishers.

Atia, M. (2007). In Whose Interest? Financial Surveillance and the Circuits of Exception in the War on Terror. *Environment and Planning D: Society and Space*, 25(3), 447–475.

Audit Magazine. (2019). IIA Quality Assessment Review: Veel ervaring veel toegevoegde waarde. *Instituut van Internal Auditors Nederland (IIA Nederland) en de Stichting Verenigde Operational Auditors (SVRO)*.

Baird, T. (2017). Knowledge of Practice: A Multi-Sited Event Ethnography of Border Security Fairs in Europe and North America. *Security Dialogue*, 48(3), 187–205.

Balázs, B. (2020). Mediated Trust: A Theoretical Framework to Address the Trustworthiness of Technological Trust Mediators. *New Media & Society*, 23(9), 2668-2690.

Balzacq, T., Basaran, T., Bigo, D., Guittet, E. P., & Olsson, C. (2010). Security practices. In *Oxford Research Encyclopedia of International Studies*.

Barry, A. (1993). The European Community and European Government: Harmonization, Mobility and Space. *Economy and Society*, 22(3), 314–326.

Barry, A. (2006). Technological Zones. *European Journal of Social Theory*, 9(2), 239–253.

Barry, A. (2012). Political Situations: Knowledge Controversies in Transnational Governance. *Critical Policy Studies*, 6(3), 324–336.

Barry, A. (2013). The Translation Zone: Between Actor-Network Theory and International Relations. Millennium: *Journal of International Studies*, 41(3), 413–429.

Basel Institute on Governance. (2017). E-learning Course Operational Analysis. https://baselgovernance.org/elearning-courses/operational-analysis-english, consulted on 17 February 2023.

Bauman, Z., & Lyon, D. (2013). *Liquid Surveillance: A Conversation*. Polity Press.

Belastingdienst. (n.d.). *Ongebruikelijke transactie melden voor de Wwft*. https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/aangifte_betalen_en_toezicht/wwft-voorkomen-van-witwassen-en-terrorismefinanciering/verplichtingen/ongebruikelijke-transactie-melden, consulted on 8 June 2021.

Belcher, O., & Martin, L. (2019). Site Visits, Selective Disclosure, and Freedom of Information in Qualitative Security Research. In M. de Goede, E. Bosma & P. Pallister-Wilkins (Eds.), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*, 33–47. Routledge.

Bellanova, R. (2014). Data Protection, With Love. *International Political Sociology*, 8(1), 112–115.

Bellanova, R. (2017). Digital, Politics, and Algorithms: Governing Digital Data Through the Lens of Data Protection. *European Journal of Social Theory*, 20(3), 329–347.

Bellanova, R., & De Goede, M. (2022). The Algorithmic Regulation of Security: An Infrastructural Perspective. *Regulation & Governance*, 16(1), 102–118.

Bellanova, R., & Duez, D. (2012). A Different View on the "Making" of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage. *European Foreign Affairs Review*, 17, 109–124.

Bellanova, R., & Fuster, G. G. (2013). Politics of Disappearance: Scanners and (Unobserved) Bodies as Mediators of Security Practices. *International Political Sociology*, 7(2), 188–209.

Bellanova, R., & Glouftsios, G. (2022). Controlling the Schengen Information System (SIS II): The Infrastructural Politics of Fragility and Maintenance. *Geopolitics*, 27(1), 160–184.

Bellanova, R., & Sætnan, A. R. (2019). How to Discomfort a Worldview? In J. P. Singh, M. Carr & R. Marlin-Bennett (Eds.), *Social Sciences, Surveillance Technologies, and Defamiliarization*, 29–40. Routledge.

Bellanova, R., Jacobsen, K. L., & Monsees, L. (2020). Taking the Trouble. Science, Technology and Security Studies. *Critical Studies on Security*, 8(2), 87-100.

Beraldo, D. & Milan, S. (2019). From Data Politics to the Contentious Politics of Data. *Big Data & Society*, 6(2).

Bernards, N., & Campbell-Verduyn, M. (2019). Understanding Technological Change in Global Finance Through Infrastructures: Introduction to Review of International Political Economy Special Issue "The Changing Technological Infrastructures of Global Finance." *Review of International Political Economy*, 26(5), 773–789.

Best, J. (2003). From the Top–Down: The New Financial Architecture and the Re-embedding of Global Finance. *New Political Economy*, 8(3), 363–384.

Best, J., & Walters, W. (2013). "Actor-Network Theory" and International Relationality: Lost (and Found) in Translation: Introduction. *International Political Sociology*, 7(3), 332–334.

Biersteker, T., & Eckert, S. (2008). *Countering the Financing of Terrorism*. Routledge.

Bigo, D., & Walker, R. B. J. (2007). Political Sociology and the Problem of the International. *Millennium: Journal of International Studies*, 35(3), 725–739.

Birchall, C. (2016). Six Answers to the Question "What is Secrecy Studies?" *Secrecy and Society*, 1(1).

Blackburn, R. (2008). The Subprime Crisis. *New Left Review*, 63–107.

Bogost, I., & Montfort, N. (2009). Platform Studies: Frequently Questioned Answers. *Digital Arts and Culture*.
Boltanski, L. (2011). *On Critique: A Sociology of Emancipation* (English edition). Cambridge: Polity Press.
Bonelli, L., & Ragazzi, F. (2014). Low-tech Security: Files, Notes, and Memos as Technologies of Anticipation. *Security Dialogue*, 45(5), 476–493.
Booth, K. (2007). *Theory of World Security*. Cambridge University Press.
Bosma, E. (2019). Multi-sited Ethnography of Digital Security Technologies. In M. de Goede, E. Bosma & P. Pallister-Wilkins (Eds.), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*, 193–212. Routledge.
Bosma, E. (2022). *Banks as Security Actors: Countering Terrorist Financing at the Human-Technology Interface*. PhD Dissertation, University of Amsterdam.
Bosma, E., De Goede, M., & Pallister-Wilkins, P. (2019). Introduction: Navigating Secrecy in Security Research. In M. de Goede, E. Bosma & P. Pallister-Wilkins (Eds.), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*, 1–27. Routledge.
Bowker, G. C., & Star, S. L. (2000). *Sorting Things Out: Classification and Its Consequences*. MIT Press.
Boy, N. (2017). Finance-Security: Where to Go? *Finance and Society*, 3(2), 208–215.
Boy, N., & Gabor, D. (2019). Collateral Times. *Economy and Society,* 48(3), 295-314.
Boy, N., Burgess, J. P., & Leander, A. (2011). The Global Governance of Security and Finance: Introduction to the Special Issue. *Security Dialogue*, 42(2), 115–122.
Boy, N., Morris, J., & Santos, M. (2017). Introduction: Taking Stock of Security and Finance. *Finance and Society*, 3(2), 102–105.
Brown, L. (1993) (Ed.) *The New Shorter Oxford English Dictionary*. Clarendon Press
Bryman, A. (2008). *Social Research Methods*. Oxford University Press.
Bueger, C., & Gadinger, F. (2014). *International Practice Theory: New Perspectives*. Palgrave Macmillan.
Bueger, C., & Gadinger, F. (2015). The Play of International Practice. *International Studies Quarterly,* 59(3), 449–460.
Buzan, B., & Hansen, L. (2010). Defining–Redefining Security. In R. A. Denemark (Ed.), *The International Studies Encyclopedia*. Blackwell Publishing.
Buzan, B., Waever, O., & De Wilde, J. (1998). *Security: A New Framework for Analysis*. Lynne Rienner.
Cakici, B., Ruppert, E., & Scheel, S. (2020). Peopling Europe Through Data Practices: Introduction to the Special Issue. *Science, Technology, & Human Values*, 45(2), 199–211.
Callon, M. (1984). Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. *The Sociological Review*, 32, 196–233.
Cheng, C. (2018). *Extralegal Groups in Post-Conflict Liberia: How Trade Makes the State*. Oxford University Press.
Collective, C. A. S. E. (2006). Critical Approaches to Security in Europe: A Networked Manifesto. *Security Dialogue*, 37(4), 443–487.
Cook, Karen. S., Hardin, R., & Levi, M. (2005). *Cooperation Without Trust*. Russell Sage Foundation.
Cutler, A. C., Haufler, V., & Porter, T. (1999). *Private Authority and International Affairs*. SUNY Press.
Dandeker, C. (2007). Surveillance: Basic Concepts and Dimensions. In S. P. Hier & J. Greenberg (Eds.), *The Surveillance Studies Reader*, 39–51. Open University Press.
De Boer, M. (2021). Beleggers reageren opgelucht na witwasboete ABN Amro. *Het Financieele Dagblad*. https://fd.nl/beurs/1380823/beleggers-reageren-opgelucht-na-witwasboete-abn-amro-qjf1caxuwzt3, consulted on 10 June 2021.
De Goede, M. (2010). Financial Security. In J. P. Burgess (Ed.), *The Routledge Handbook of New Security Studies*, Chapter 11, 100–109. Routledge.
De Goede, M. (2012). *Speculative Security: The Politics of Pursuing Terrorist Monies*. University of Minnesota Press.
De Goede, M. (2017a). *Banks in the Frontline: Assembling Space/Time in Financial Warfare*. In B. Christophers, A. Leyshon, & G. Mann (Eds.), Money and Finance After the Crisis, 17–144. John Wiley & Sons, Ltd.
De Goede, M. (2017b). Chains of Securitization. *Finance and Society*, 3(2), 197–207.
De Goede, M. (2018). The Chain of Security. *Review of International Studies*, 44(1), 24–42.
De Goede, M. (2020). Engagement All the Way Down. *Critical Studies on Security*, 8(2), 101-115.
De Goede, M. (2021). Finance/Security Infrastructures. *Review of International Political Economy*, 28(2), 351–

368.
De Goede, M., & Westermeier, C. (2022). Infrastructural Geopolitics. *International Studies Quarterly*, 66(3), 1-12.
De Goede, M., Bosma, E., & Pallister-Wilkins, P. (Eds.) (2019). *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*. Routledge.
De Oliveira, I. S. (2018). The Governance of the Financial Action Task Force: An Analysis of Power and Influence Throughout the Years. *Crime, Law and Social Change*, 69(2), 153–172.
De Vries, G. (2016). *Bruno Latour*. Polity Press.
De Wilde, M. (2020). A Care-Infused Market Tale: On (Not) Maintaining Relationships of Trust in Energy Retrofit Products. *Journal of Cultural Economy*, 13(5), 561–578.
Dehouck, M., & De Goede, M. (2021). *Public-Private Financial Information-Sharing Partnerships in the Fight Against Terrorism Financing*. University of Amsterdam.
Denis, J., & Pontille, D. (2019). Why Do Maintenance and Repair Matter? In A. Blok, I. Farías, & C. Roberts (Eds.), *The Routledge Companion to Actor-Network Theory*, 283–293. Routledge.
Desrosières, A. (1998). *The Politics of Large Numbers: A History of Statistical Reasoning*. Harvard University Press.
Dijstelbloem, H., & Pelizza, A. (2019). The State Is the Secret: For a Relational Approach to the Study of Border and Mobility Control in Europe. In M. de Goede, E. Bosma, & P. Pallister-Wilkins (Eds.), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*, 48–62. Routledge.
Dijstelbloem, H., & Walters, W. (2021). Atmospheric Border Politics: The Morphology of Migration and Solidarity Practices in Europe. *Geopolitics*, 26(2), 497–520.
DNB, [De Nederlandse Bank]. (2019). *Convenant Terrorismefinanciering Taskforce*. https://zoek.officielebekendmakingen.nl/stcrt-2019-43628.html, consulted on 8 June 2021.
DNB, [De Nederlandse Bank]. (2020). *Leidraad Wwft en Sw Versie December 2020*.
Draku, F. (2020). The HoFIUs Communicate on a Daily Basis Through the Egmont Secure Web and Meet Once a Year in the Egmont Group Annual Plenary. *Monitor*. https://www.monitor.co.ug/uganda/special-reports/elections/govt-freezes-accounts-of-4-ngos-doing-poll-work-3216360, consulted 25 June 2021.
Durner, T., & Shetret, L. (2015). *Understanding Bank De-risking and its Effects on Financial Inclusion: An Exploratory Study* [Research Report]. Global Center on Cooperative Security & Oxfam International.
Egmont Group. (2013). *Principles for Information Exchange Between FIUs*. The Egmont Group of FIUs.
Egmont Group. (2015). *20 Years Annual Report 2014-2015: From 13 to 151 FIUs in 20 Years*. Egmont Group of FIUs.
Egmont Group. (2017). *Operational Guidance for FIU Activities and the Exchange of Information*. The Egmont Group of FIUs.
Egmont Group. (2018). *Annual Report 2017/2018*. Egmont Group of FIUs.
Egmont Group. (2019). *Egmont Group of FIUs Charter*. The Egmont Group of FIUs.
Egmont Group. (2021a). *Annual Report 2019/2020*. Egmont Group of FIUs.
Egmont Group. (2021b). *Egmont Group Chair's Statement on Allegations of FIUs Misusing their Powers to Combat ML and TF.* https://egmontgroup.org/en/content/egmont-group-chair%E2%80%99s-statement, consulted July 6 2021.
Egmont Group. (2022a). Organisation and Structure. *Egmont Group*. https://egmontgroup.org/about/organization-and-structure/, consulted 4 August 2022.
Egmont Group. (2022b). About the Egmont Group. *Egmont Group*. https://egmontgroup.org/about/, consulted 4 August 2022.
Epstein, S. (2009). Beyond the Standard Human? In M. Lampland & S. L. Star (Eds.), *Standards and their Stories: How Quantifying, Classifying, and Formalizing Practices Shape Everyday Life*. Chapter 2, 35–53. Cornell University Press.
Eriksen, T. H. (2010). *Small Places, Large Issues: An Introduction to Social and Cultural Anthropology*. Pluto Press.
EU-FIU Platform. (2016). *Mapping Exercise and Gap Analysis on FIUs Powers and Obstacles for Obtaining and Exchanging Information*. Brussels.
EU-FIU Platform. (2017). *Annex to EU FIUs' Platform Minutes (34th Meeting 11-12 December 2017), Europol Report on "From Suspicion to Action – Converting Financial Intelligence into Greater Operational Im-*

pact", Preliminary Overview of Main Issues.
European Commission. (2015a). *25th Meeting of the EU FIUs PLATFORM 1 June 2015*.
European Commission. (2015b). *26th Meeting of the EU FIUs PLATFORM 16 October 2015*.
European Commission. (2016). *Gedelegeerde Verordening (EU) 2016/1675 van de Commissie*. https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:02016R1675-20181022&from=EN, consulted on 6 May 2021.
European Commission. (2016a). *27th Meeting of the EU FIUs PLATFORM 26 January 2016*.
European Commission. (2016b). *28th Meeting of the EU FIUs PLATFORM 12 May 2016*.
European Commission. (2016c). *29th Meeting of the EU FIUs PLATFORM 10 June 2016*.
European Commission. (2017). *Commission Staff Working Document: On Improving Cooperation Between EU FIUs*.
European Commission. (2017a). *32nd Meeting of the EU FIUs PLATFORM 29 -30 March 2017*.
European Commission. (2017b). *33rd Meeting of the EU FIUs PLATFORM 20 -21 September 2017*.
European Commission. (2017c). *Commission Staff Working Document: On Improving Cooperation Between EU FIUs*. Brussels.
European Commission. (2018). *36th Meeting of the EU FIUs PLATFORM 7 June 2018*.
European Commission. (2019). *39th Meeting of the EU FIUs PLATFORM - DRAFT AGENDA*.
European Commission. (2022). *EU FIUs' Platform (E03251)*. https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3251, consulted 4 August 2022.
Europol. (2017). *From Suspicion to Action: Converting Financial Intelligence into Greater Operational Impact*. Publications Office of the European Union.
Fahey, E. & Curtin, D. (Eds.) (2014). *A Transatlantic Community of Law: Legal Perspectives On the Relationship Between the EU and US Legal Orders*. Cambridge University Press.
FATF. (2001). *FATF IX Special Recommendations*. https://www.fatf-gafi.org/documents/documents/ixspecialrecommendations.html, consulted August 4 2022.
FATF. (2012). *Operational Issues Financial Investigations Guidance*. Financial Action Task Force.
FATF. (2015). *Guidance on AML/CFT-related Data and Statistics*. Financial Action Task Force.
FATF. (2020b). [Letter to the UN Office of the High Commissioner for Human Rights]. Retrieved online from: https://fatfplatform.org/assets/2020-12-18-FATF-re-UN-APML-Serb.pdf, consulted 5 August 2022.
FATF. (2022). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. Financial Action Task Force.
FATF. (n.d.). *Who We Are*. https://www.fatf-gafi.org/about/, consulted 4 August 2022.
Ferrari, V. (2020). Crosshatching Privacy: Financial Intermediaries' Data Practices Between Law Enforcement and Data Economy. *European Data Protection Law Review*, 6(4), 522–535.
FIU-Nederland. (2019). *FIU-Nederland Jaaroverzicht 2018*. https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/fiu-nederland_jaaroverzicht_2018_nl_web.pdf, consulted on 5 August 2022.
FIU-Nederland. (2020). *FIU-Nederland Jaaroverzicht 2019*. https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/jaaroverzicht_2019_-_fiu_nederland.pdf, consulted on 5 August 2022.
FIU-Nederland. (2020). *FIU-the Netherlands Annual Review 2019*. FIU-the Netherlands. https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/fiu-nederland_jaaroverzicht_2018_nl_web.pdf, consulted on 5 August 2022.
FIU-Nederland. (2021*). *FIU-Nederland Jaaroverzicht 2020*. https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/5169-fiu_jaaroverzicht_2020nl_web_v3.pdf, consulted on 5 August 2022.
FIU-Nederland. (n.d.). *Handleiding GoAML*. https://meldportaal.fiu-nederland.nl/public_documents/Handleiding%20goAML%20Nederlands%20release%204%200%20(nieuw).pdf, consulted on 5 August 2022.
FIU-Nederland. (n.d.a). *Banken*. https://www.fiu-nederland.nl/nl/meldergroep/8, consulted on 8 June 2021.
FIU-Nederland. (n.d.b). *Ben ik meldplichtig*? https://www.fiu-nederland.nl/nl/melden/ben-ik-meldplichtig, consulted on 5 May 2021.
FIU-Nederland. (n.d.c). *Casuïstiek*. https://www.fiu-nederland.nl/nl/wetgeving/casuistiek, consulted on 18 May 2021.
FIU-Nederland. (n.d.d). *Handleiding GoAML*. https://meldportaal.fiu-nederland.nl/public_documents/Handleiding%20goAML%20Nederlands%20release%204%200%20(nieuw).pdf, consulted on 4 August 2022.

FIU-Nederland. (n.d.e). Moet ik rekening houden met de Algemene Verordening Gegevensbescherming (AVG) bij het nakomen van de verplichtingen op grond van de Wet ter Voorkoming van Witwassen en Financieren van Terrorisme (Wwft)? https://www.fiu-nederland.nl/nl/faq#n1222, consulted on 4 January 2022.

FIU-Nederland. (n.d.f). *Organisatie*. https://www.fiu-nederland.nl/nl/over-fiu/organisatie, consulted on 8 June 2021.

Floyd, R. (2007). Human Security and the Copenhagen School's Securitization Approach. *Human Security Journal*, 5(37), 38–49.

Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*. Vintage Books.

Fox, N. J. (2011). Boundary Objects, Social Meanings and The Success Of New Technologies. *Sociology* 45(1), 70–85.

Friedman, T. (2005). *The World is Flat: A Brief History of the Globalized World in the 21st Century*. Farrar, Straus and Giroux.

Geertz, C. (1973). *The Interpretation of Cultures*. Basic Books.

Gilbert, E. (2015). Money as a "Weapons System" and the Entrepreneurial Way of War. *Critical Military Studies*, 1(3), 202–219.

Gilbert, E. (2015a) The Gift of War: Cash, Counterinsurgency and "Collateral Damage," *Security Dialogue,* 46(5), 403-421.

Gilbert, E. (2017). Militaries, Finance, and (In)security. *Finance and Society*, 3(2), 180–187.

Gillespie, T. (2010). The Politics of "Platforms". *New Media & Society*, 12(3), 347–364.

Gillespie, T. (2014). *The Relevance of Algorithms*. In T. Gillespie, P. J. Boczkowski, & K. A. Foot (Eds.), Media Technologies: Essays on Communication, Materiality, and Society. 167–193. MIT Press.

Gitelman, L., & Jackson, V. (2013). Introduction. In L. Gitelman (Ed.), *"Raw Data" is an oxymoron*, 1–14. MIT Press.

Glaser, B. G., & Holton, J. (2004). Remodeling Grounded Theory. 5(2), Article 2.

Glaser, B. G., & Strauss, A. L. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine Transation.

Gusterson, H. (2008). Ethnographic Research. In A. Klotz & D. Prakash (Eds.), *Qualitative Methods in International Relations*, 93-113. Palgrave.

Haggerty, K. D., & Ericson, R. V. (2000). The Surveillant Assemblage. *British Journal of Sociology*, 51(4), 605–622.

Hansen, H. K., & Porter, T. (2012). What Do Numbers Do. In Transnational Governance? *International Political Sociology*, 6(4), 409–426.

Harman, G. (2009). *Prince of Networks: Bruno Latour and Metaphysics*. re.press.

Helgesson, K. S., & Mörth, U. (2019). Instruments of Securitization and Resisting Subjects: For-Profit Professionals In the Finance–Security Nexus. *Security Dialogue*, 50(3), 257–274.

Hendrikse, R., Bassens, D., & Van Meeteren, M. (2018). The Appleization of Finance: Charting Incumbent Finance's Embrace of FinTech. *Finance and Society*, 4(2), 159–180.

Heng, Y., & Mcdonagh, K. (2008). The Other War on Terror Revealed: Global Governmentality and the Financial Action Task Force's Campaign Against Terrorist Financing. *Review of International Studies,* 34(3), 553–573.

Ho, K. (2009). *Liquidated: An Ethnography of Wall Street*. Duke University Press.

Ho, K. (2012). "*Studying up" Wall Street: Reflections on Theory and Methodology*. In L. Aguiar & C. Schneider (Eds.), Researching Amongst Elites: Challenges and Opportunities in Studying up. Ashgate Publishing.

Hoffman, A. M. (2002). A Conceptualization of Trust In International Relations. *European Journal of International Relations*, 8(3), 375–401.

Hoijtink, M. (2017). Governing in the Space of the "Seam": Airport Security After the Liquid Bomb Plot. *International Political Sociology,* 11(3), 308-326.

Hoijtink, M. (2019). Gender, Ethics and Critique in Researching Security and Secrecy. In M. de Goede, E. Bosma, & P. Pallister-Wilkins (Eds.), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*, 143-157. Routledge.

Hoijtink, M., & Leese, M. (Eds.). (2019). *Technology and Agency in International Relations*. Routledge.

Holtrop, T. (2017). 6.15%: Taking Numbers at Interface Value. *Science & Technology Studies,* 31(4), 75–88.

Hülsse, R., & Kerwer, D. (2007). Global Standards in Action: Insights from Anti-Money Laundering Regulation.

Organization, 14(5), 625–642.
Huysmans, J. (2006). *The Politics of Insecurity: Fear, Migration and Asylum in the EU*. Routledge.
Huysmans, J. (2011). What's in an Act? On Security Speech Acts and Little Security Nothings. *Security Dialogue*, 42(4–5), 371–383.
Iafolla, V. (2018). The Production of Suspicion in Retail Banking: An Examination of Unusual Transaction Reporting. In C. King, C. Walker, & J. Gurule (Eds.), *The Palgrave Handbook of Criminal and Terrorism Financing Law*, 81–107. Springer International Publishing.
IMF and WB. (2004). *FIUs: An Overview*. International Monetary Fund Publication Services.
İşleyen, B. (2018). Turkey's Governance of Irregular Migration at European Union Borders: Emerging Geographies of Care and Control. *Environment and Planning D: Society and Space*, 36(5), 849–866.
Issa, H. (2021). NGOs Plead with Government Over Frozen Bank Accounts. *URN*. https://ugandaradionetwork.net/story/ngos-plead-with-government-over-frozen-bank-accounts, consulted 25 June 2021.
Jakobi, A. P. (2018). Governing Illicit Finance in Transnational Security Spaces: The FATF and Anti-Money Laundering. *Crime, Law and Social Change*, 69(2), 173–190.
Janssen, R. (2022). Pakkans? 0,083 procent. *De Groene Amsterdammer*. https://www.groene.nl/artikel/pakkans-0-083-procent, consulted 5 August 2022.
Jasanoff, S. (2004). *States of Knowledge: The Co-Production of Science and the Social Order*. Routledge.
Jones, G. M. (2014). Secrecy. *Annual Review of Anthropology*, 43(1), 53–69.
Kamphuis, B. (2021). Een miljoen "ongebruikelijke" transacties, maar weinig aanhoudingen. *NOS*. https://nos.nl/nieuwsuur/artikel/2403990-een-miljoen-ongebruikelijke-transacties-maar-weinig-aanhoudingen, consulted on 4 December 2021.
Kazansky, B. (2021). "It Depends on Your Threat Model": The Anticipatory Dimensions of Resistance to Data-Driven Surveillance. *Big Data & Society*, 8(1), 1–12.
Kazibwe, K. (2021). Govt Unfreezes Accounts of NGOs Accused of Terrorism Funding. *NilePost*. https://nilepost.co.ug/2021/02/27/govt-unfreezes-accounts-of-ngos-accused-of-terrorism-funding/, consulted 25 June 2021.
KLPD, [Korps Landelijke Politiediensten]. (2008). Witwassen: Verslag van een onderzoek voor het nationaal dreigingsbeeld 2008. https://docplayer.nl/1602433-Witwassen-verslag-van-een-onderzoek-voor-het-nationaal-dreigingsbeeld-2008-klpd-dienst-ipol.html
Koole, B. (2020). Trusting to Learn and Learning to Trust. A Framework for Analyzing the Interactions of Trust and Learning in Arrangements Dedicated to Instigating Social Change. *Technological Forecasting & Social Change*, 161, 120260.
Krippner, G. R. (2005). The Financialization of the American Economy. *Socio-Economic Review*, 173–208.
Kroon, U. (2013). Ma3tch: Privacy and Knowledge: "Dynamic Networked Collective Intelligence". *2013 IEEE International Conference on Big Data*, 23–31. http://ieeexplore.ieee.org/document/6691683/
Lababidi, E. M. R. (2020). State and Institutional Capacity in Combating Money Laundering and Terrorism Financing in Armed Conflict: The Central Bank of Syria. *Journal of Money Laundering*, 23(1), 155-172.
Laet, M. de, & Mol, A. (2000). The Zimbabwe Bush Pump: Mechanics of a Fluid Technology. *Social Studies of Science*, 30(2,), 225–263.
Lagerwaard, P. (2015). Negotiating Global Finance: Trading on Dalal Street, Mumbai. *Journal of Cultural Economy*, 8(5), 564–581.
Lagerwaard, P. (2018) *Following Suspicious Transactions in Europe: Comparing the Operations of European FIUs (FIUs)*. FOLLOW Research Report. Amsterdam Institute for Social Science Research (AISSR).
Lagerwaard, P. (2020). Flattening the International: Producing Financial Intelligence Through a Platform. *Critical Studies on Security*, 8(2), 160–174.
Lagerwaard, P. (2022). Financiële Surveillance en de rol van de Financial Intelligence Unit in Nederland. *Beleid en Maatschappij* 49(2), 128-153.
Lampland, M., & Star, S. L. (2009). Reckoning with Standards. In M. Lampland & S. L. Star (Eds.), *Standards and their Stories: How Quantifying, Classifying, and Formalizing Practices Shape Everyday Life*, Chapter 1, 3–24. Cornell University Press.
Langenohl, A. (2017a). Modular Sovereignty, Security and Debt: The Excessive Deficit Procedure of the European Union. *Finance and Society*, 3(2), 124–142.
Langenohl, A. (2017b). Securities Markets and Political Securitization: The Case of the Sovereign Debt Crisis in

the Eurozone. *Security Dialogue*, 48(2), 131–148.
Langenohl, A. (2021). Securing the Separation Between State and Finance: Entanglements Between Securitization and Societal Differentiation. *Review of International Political Economy*, 29(5), 1–20.
Langley, P. (2007). Uncertain Subjects of Anglo-American Financialization. *Cultural Critique*, 65, 67–91.
Langley, P. (2014). *Liquidity Lost: The Governance of the Global Financial Crisis*. Oxford University Press.
Langley, P. (2017). Finance/Security/Life. *Finance and Society*, 3(2), 173–179.
Latour, B. (1987). *Science in Action: How to Follow Scientists and Engineers Through Society*. Harvard University Press.
Latour, B. (1999). *Pandora's Hope: Essays on the Reality of Science Studies*. Harvard University Press.
Latour, B. (2007). *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford University Press.
Latour, B. (2010). An Attempt at a "Compositionist Manifesto." *New Literary History*, 41, 471–490.
Latour, B. (2017). *Facing Gaia: Eight Lectures on the New Climatic Regime*. Polity Press.
Latour, B. (2018). *Down to Earth: Politics in the New Climatic Region*. Polity Press.
Latour, B. (2021). *After Lockdown: A Metamorphosis*. Polity Press.
Law, J. (1986). On the Methods of Long-Distance Control: Vessels, Navigation and the Portuguese Route to India. *The Sociological Review*, 32, 234–263.
Law, J. (2002). Objects and Spaces. *Theory, Culture & Society*, 19(5/6), 15.
Law, J. (2004). *After Method: Mess in Social Science Research*. Routledge.
Law, J. (2016). STS as Method. In U. Felt, R. Fouché, C. A. Miller, & L. Smith-Doerr (Eds.), *Handbook of Science and Technology Studies* (4th ed.), 31–58. MIT Press.
Leander, A. (Ed.) (2013). *Commercialising Security in Europe: Political Consequences for Peace Operations*. Routledge.
Leander, A. (2015a). Ethnographic Contributions to Method Development: "Strong Objectivity" in Security Studies. *International Studies Perspectives*, 17(4), 462-475.
Leander, A. (2015b). Theorising International Monetary Relations: Three Questions about the Significance of Materiality. *Contexto Internacional*, 37(3), 945-973.
Leander, A. (2021). Locating (new) Materialist Characters and Processes in Global Governance. *International Theory*, 13(1), 157-168.
Leonelli, S. (2016). *Data-Centric Biology: A Philosophical Study*. University of Chicago Press.
Levi, R., & Valverde, M. (2008). Studying Law by Association: Bruno Latour Goes to the Conseil d'Etat. *Law & Social Inquiry*, 33(3), 805–825.
Leyshon, A., & Thrift, N. (1997). *Money/Space: Geographies of Monetary Transformation*. Routledge.
Liss, C., & Sharman, J. (2015). Global Corporate Crime-Fighters: Private Transnational Responses to Piracy and Money Laundering. *Review of International Political Economy: RIPE*, 22(4), 693–718.
Löwenheim, O. (2015). Bicycle. In M. B. Salter (Ed.), *Making Things International 1: Circuits and Motion*, 72-84. University of Minnesota Press.
Lupton, D. (2012). M-health and Health Promotion: The Digital Cyborg and Surveillance Society. *Social Theory & Health*, 10(3), 229–244.
Lyon, D. (2007). *Surveillance Studies: An Overview*. Polity Press.
Lyon, D., Haggerty, K. D., & Ball, K. (2012). Introduction Surveillance Studies. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge Handbook of Surveillance Studies*, 1–12). Routledge.
Mackenzie, D. (2001). *Mechanizing Proof: Computing, Risk, and Trust*. MIT Press.
Marcus, G. E. (1995). Ethnography in/of the World System: The Emergence of Multi-Sited Ethnography. *Annual Review of Anthropology*, 24, 95–117.
Marston, S., A., Jones III, J., P., & Woodward, K. (2005). Human Geography without Scale. *Transactions of the Institute of British Geographers*, 30(4), 416–432.
Marx, G. (2012). "Your papers please": Personal and Professional Encounters with Surveillance. In K Bal, K. Haggerty & D. Lyon (Eds.), *Routledge Handbook of Surveillance Studies*, Preface xx-xxxi. Routledge.
McAdams, D. P. (2011). Exploring Psychological Themes Through Life-Narrative Accounts. In J. A. Holstein & J. F. Gubrium (Eds.), *Varieties of Narrative Analysis*. Sage Publications.
MENA FATF. (2018). *Mutual Evaluation Report: 13th Follow-up Report for Syria*. Retrieved from MENA FATF Website: http://www.menafatf.org/mutual-evaluations-follow/follow-up-reports.
Mendoza, R. (2016). Photography Tips. *Outside the Lens*. https://outsidethelens.org/post.php?s=2016-04-02-

photography-tips, consulted 12 September 2022.
Michael, M. (2016). *Actor-Network Theory: Trials, Trails and Translations*. Sage Publications.
Milan, S. (2019). Acting on Data(fication). In H. Stephansen & E. Treré (Eds.*), Citizen Media and Practice: Currents, Connections, Challenges*, 212-226. Routledge.
Ministry of Justice, Netherlands. (2008). Wet ter Voorkoming van Witwassen en Financieren van Terrorisme (Wwft).
Mitsilegas, V. (2014). Transatlantic Counterterrorism Cooperation and European values: The Elusive Quest for Coherence. In E. Fahey & D. Curtin (Eds.), *A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US Legal Orders*, 289-315. Cambridge University Press.
Mitsilegas, V., & Vavoula, N. (2016). The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law. *Maastricht Journal of European and Comparative Law*, 23(2), 261–293.
Mol, A. (1999). Ontological Politics. A Word and Some Questions. *The Sociological Review*, 47(1l), 74–89.
Mol, A. (2002). *The Body Multiple: Ontology in Medical Practice*. Duke University Press.
Mol, A. (2010). Actor-Network Theory: Sensitive Terms and Enduring Tensions. *Kölner Zeitschrift für Soziologie und Sozialpsychologie. Sonderheft*, 50(1), 253–269.
Mol, A. (2015). A Reader's Guide to the "Ontological Turn", Part 4, *Science, Medicine, and Anthropology*, 5.
Monsees, L. (2020). "A War Against Truth"—Understanding the Fake News Controversy. *Critical Studies on Security*, 8(2), 116–129.
Mouzakiti, F. (2020). Cooperation Between FIUs in the European Union: Stuck in the Middle Between the General Data Protection Regulation and the Police Data Protection Directive. *New Journal of European Criminal Law*, 11(3), 351–374.
Mouzakiti, F. (2020). Cooperation Between FIUs in the European Union: Stuck in the Middle Between the General Data Protection Regulation and the Police Data Protection Directive. *New Journal of European Criminal Law*, 11(3), 351–374.
Mügge, D. (Ed.) (2014). *Europe and the Governance of Global Finance*. Oxford University Press.
Mügge, D. (2015). Studying Macroeconomic Indicators as Powerful Ideas. *Journal of European Public Policy,* 23(3), 410-427.
Mügge, D. (2020). International Economic Statistics: Biased Arbiters in Global Affairs? *Fudan Journal of the Humanities and Social Sciences*, 13(1), 93–112.
Mutlu, C. E., & Salter, M. B. (Eds.). (2014). Commensurability of Research Methods in Critical Security Studies. *Critical Studies on Security*, 2(3), 353–355.
Nadrous, F. (2020). Tienduizenden witwasmeldingen, amper strafzaken. "Soms lijkt het of het hele meldsysteem voor niets is". *Trouw*. https://www.trouw.nl/economie/tienduizenden-witwasmeldingen-amper-strafzaken-soms-lijkt-het-of-het-hele-meldsysteem-voor-niets-is~b03c7f64/, consulted on June 8 2021.
Nance, M. T. (2018). The Regime That FATF Built: An Introduction to the Financial Action Task Force. *Crime, Law and Social Change*, 69(2), 109–129.
Nu.nl. (2007). Politie kan criminelen "googelen". *Nu.nl*. https://www.nu.nl/internet/1106457/politie-kan-criminelen-googelen.html, consulted
Olsen, R. A. (2008). Trust as Risk and the Foundation of Investment Value. *The Journal of Socio-Economics*, 37(6), 2189–2200.
Opitz, S., & Tellmann, U. (2015). Europe as Infrastructure: Networking the Operative Community. *South Atlantic Quarterly*, 114(1), 171–190.
Orsini, A., Louafi, S., & Morin, J.-F. (2017). Boundary Concepts for Boundary Work Between Science and Technology Studies and International Relations. *Review of Policy Research*, 34(6), 734–743.
Orwell, G. (1949). *Nineteen Eighty-Four*. Penguin Books.
Overton, J. (1999) Worlds Apart: Reflections on Trust, Colonialism and Decolonisation, *Hume Papers on Public Policy,* 7, 33-41.
Pallister-Wilkins, P. (2016). How Walls do Work: Security Barriers as Devices of Interruption and Data Capture. *Security Dialogue*, 47(2), 151–164.
Pelizza, A. (2016). Developing the Vectorial Glance: Infrastructural Inversion for the New Agenda on Government Information Systems. *Science, Technology, & Human Values*, 41(2), 298–321.
Permanent Mission of the Republic of Serbia to the United Nations (2020). *Responses of the Republic of Ser-*

bia. https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=35826. Consulted 17 February 2023.

Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook. *New Media & Society*, 20(1), 293–310.

Pols, J. (2005). Enacting Appreciations: Beyond the Patient Perspective. *Health Care Analysis*, 13(3), 203–221.

Porter, T. M. (1996). *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life*. Princeton University Press.

Pryke, M. (2010). Money's Eyes: The Visual Preparation of Financial Markets. *Economy and Society*, 39(4), 427–459.

Rasha, M. (2019). *Syria Participates in Egmont Group for Combating Money Laundering and Terrorism Funding in Hague*. SANA. https://www.sana.sy/en/?p=169229, consulted 17 March 2021.

RIEC-LIEC. (2020). RIEC-LIEC Jaarverslag 2019. https://www.riec.nl/documenten/jaarverslagen/2019/06/23/riec-liec-jaarverslag-2019, , consulted 5 August 2022.

Riemslag Baas, A. M. (2021). De bijdrage van banken aan het voorkomen en bestrijden van witwassen en terrorismefinanciering. *Tijdschrift Financieel Recht in de Praktijk*, 1, 45–51.

Rocha de Siqueira, I. (2017). Development by Trial and Error: The Authority of Good Enough Numbers. *International Political Sociology*, (11), 166–184.

Rose, N. (1991). Governing by Numbers: Figuring out Democracy. *Accounting, Organizations and Society*, 16(7), 673–692.

Rothe, D. (2020). Jellyfish Encounters: Science, Technology and Security in the Anthropocene Ocean. *Critical Studies on Security*, 8(2), 145–159.

Rutten, M. (2007). "*Leuke vakantie gehad?": Verhalen over antropologisch veldwerk*. Aksant.

Salter, M. B. (ed.) (2008). *Politics at the Airport*. University of Minnesota Press.

Salter, M. B. (2010). *Surveillance*. In J. P. Burgess (Ed), The Routledge Handbook of New Security Studies,187–196. Routledge.

Salter, M. B. (2015). *Making Things International 1: Circuits and Motion*. University of Minnesota Press.

Salter, M. B. (2016). *Making Things International 2: Catalysts and Reactions*. University of Minnesota Press.

Salter, M. B., & Mutlu, C. E. (2013). *Research Methods in Critical Security Studies: An Introduction*. Routledge.

Salter, M. B., & Walters, W. (2016). Bruno Latour Encounters International Relations: An Interview. *Millennium: Journal of International Studies*, 44(3), 524–546.

Salter, M. B., Cohn, C., Neal, A. W., Wibben, A. T., Burgess, J. P., Elbe, S., Austin, J. L., Huysmans, J., Walker, R., Wæver, O., Williams, M. C., Gilbert, E., Frowd, P. M., Rosenow, D., Oliveira Martins, B., Jabri, V., Aradau, C., Leander, A., Bousquet, A., Hansen, L. (2019). Horizon Scan: Critical Security Studies for the Next 50 years. *Security Dialogue*, 50(4_suppl), 9–37.

Scheel, S., Ruppert, E., & Ustek-Spilda, F. (2019). Enacting Migration through Data Practices. *Environment and Planning D: Society and Space*, 37(4), 579–588.

Schmid, A. (2004). Terrorism - The Definitional Problem. *Case W. Res. J. Int'l L.*, 36(2), 375–419.

Schneider, A. (2003). On "Appropriation". A Critical Reappraisal of the Concept and its Application in Global Art Practices. *Social Anthropology*, 11(2), 215–229.

Schouten, P. (2014). Security as Controversy: Reassembling Security at Amsterdam Airport. *Security Dialogue*, 45(1), 23–42.

Searle, R. H., Nienaber, A.-M. I., & Sitkin, S. B. (Eds.). (2018). *The Routledge Companion to Trust*. Routledge.

Shapiro, M. J. (2015). Tanks. In M. B. Salter (Ed.), *Making Things International 1: Circuits and Motion*, 212-221. University of Minnesota Press.

Sharman, J. C. (2008). Power and Discourse in Policy Diffusion: Anti-Money Laundering in Developing States. *International Studies Quarterly*, 52(3), 635–656.

Sharman, J. C. (2009). The Bark Is the Bite: International Organizations and Blacklisting. *Review of International Political Economy*, 16(4), 573–596.

Sieckmann, J. (2018). Proportionality as a Universal Human Rights Principle. In D. Duarte & J. Silva Sampaio (Eds.), *Proportionality in Law*, 3–24. Springer International Publishing.

Sitkin, S. B., & Bijlsma-Frankema, K. M. (2018). Distrust. In R. H. Searle, A.-M. I. Nienaber, & S. B. Sitkin (Eds.*), The Routledge Companion to Trust*, 128-150. Routledge.

Siu, L. L. S. (2010). Gangs in the Markets: Network-based Cognition in China's Futures Industry. *International*

Journal of China Studies, 1(2), 21.
Sorel, J.-M. (2003). Some Questions About the Definition of Terrorism and the Fight Against Its Financing. *European Journal of International Law*, 14(2), 365–378.
Spradley, J. P. (1980). *Participant Observation*. Holt, Rinehart and Winston.
Star, S. L. (1990). Power, Technology and the Phenomenology of Conventions: On being Allergic to Onions. *The Sociological Review*, 38(1_suppl), 26–56.
Star, S. L. (1999). The Ethnography of Infrastructure. *American Behavioral Scientist*, 43(3), 377–391.
Star, S. L. (2010). This is Not a Boundary Object: Reflections on the Origin of a Concept. *Science, Technology, & Human Values*, 35(5), 601–617.
Star, S. L., & Griesemer, J. (1989). Institutional Ecology, "Translations" and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39. *Social Studies of Science*, 19(3), 387–420.
Star, S. L., & Ruhleder, K. (1996). Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. *Information Systems Research*, 7(1), 111–134.
Stengers, I. (2000). *The Invention of Modern Science*. University of Minnesota Press.
Swanborn, P. G. (2012). *Case–Study's: Wat, wanneer en hoe?* Boom.
The Independent. (2021). *EU, US envoys urge gov't to unfreeze CSO bank accounts*. The Independent. https://www.independent.co.ug/eu-us-envoys-urge-govt-to-unfreeze-cso-bank-accounts/, consulted 25 June 2021.
Timan, T., & Grommé, F. (2020). Wat is rechtvaardige AI?: Een kader voor het ontwikkelen en toepassen van algoritmes voor automatische besluitvorming. *Beleid en Maatschappij*, 47(4), 425–438.
Tsing, A. L. (2005). *Friction: An Ethnography of Global Connection*. Princeton University Press.
Tsing, A. L. (2015). *The Mushroom at the End of the World: On the Possibility of Life in Capitalist Ruins*.Princeton University Press.
Tweede Kamer der Staten-Generaal (1998). Uitwisseling van Recherche-informatie tussen CRI en Politieregio's. https://zoek.officielebekendmakingen.nl/kst-26215-4.pdf, consulted 5 August 2022.
Van der Kist, J., Dijstelbloem, H., & De Goede, M. (2019). In the Shadow of Asylum Decision-Making: The Knowledge Politics of Country-of-Origin Information. *International Political Sociology*, 13(1), 68–85.
Van Dijck, J. (2014). Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. *Surveillance & Society*, 12(2), 197–208.
Van Oorschot, I. (2020). *The Law Multiple: Judgment and Knowledge in Practice*. Cambridge University Press.
Vedrenne, G. (2021). EXCLUSIVE: Egmont Flags Government Abuse of Financial Intelligence. *ACAMS moneylaundering.com*. https://www.moneylaundering.com/news/exclusive-egmont-flags-government-abuse-of-financial-intelligence/, consulted 2 December 2022.
Vijayakumar, G. (2022). Vantage Point in Photography - Complete Guide with Examples. *Photography Axis*. https://www.photographyaxis.com/photography-articles/vantage-point-photography/, consulted on 12 September 2022.
VIRBI. (2013). *Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013*. https://wetten.overheid.nl/BWBR0033507/2013-06-01, consulted on 8 June 2021.
Vlcek, W. (2007). Surveillance to Combat Terrorist Financing in Europe: Whose Liberty, Whose Security? *European Security*, 16(1), 99–119.
Vlcek, W. (2009). Hitting the Right Target: EU and Security Council Pursuit of Terrorist Financing. *Critical Studies on Terrorism*, 2(2), 275–291.
Vlcek, W. (2012). Power and the Practice of Security to Govern Global Finance. *Review of International Political Economy*, 19(4), 639–662.
Walker, R. B. J. (2006). Lines of Insecurity: International, Imperial, Exceptional. *Security Dialogue*, 37(1), 65–82.
Walters, W. (2014). Drone Strikes, Dingpolitik and Beyond: Furthering the Debate on Materiality and Security. *Security Dialogu*e, 45(2), 101–118.
Weller, T. (2012). The Information State: An Historical Perspective on Surveillance. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge Handbook of Surveillance Studies*, 57–63. Routledge.
Wesseling, M. (2013). *The European Fight against Terrorism Financing: Professional Fields and New Governing Practices*. PhD Dissertation, University of Amsterdam.
Wesseling, M. (2018). Een effectief beleid tegen terrorismefinanciering: Tijd voor een eerlijk gesprek. *De Com-*

plience Officer, 8(28), 16–19.

Westermeier, C. (2019). Political Security and Finance – A Post-Crisis and Post-Disciplinary Perspective. *Zeitschrift f*ür Politikwissenschaft, 29(1), 105–122.

Westermeier, C. (2020). Money is Data – the Platformization of Financial Transactions. *Information, Communication & Society,* 23(14), 2047-2063.

Williams, M. C. (2010). The Public, the Private and the Evolution of Security Studies. *Security Dialogue*, 41(6), 623–630.

Zelizer, V. A. (2006). Circuits in Economic Life. *Economic Sociology*, 8(1), 30–35.

Zelizer, V. A. (2004). Circuits of Commerce. In J. C. Alexander, G. T. Marx, & C. L. Williams (Eds.), *Self, Social Structure, and Beliefs*, 122-144. University of California Press.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books Ltd.

Annex A: List of Respondents

For anonymization purposes, the name, organization, nationality, and gender have not been included. In-text citations refer to the role and interview date.

Number	Role	Type of interview	Time	Recorded
1	Two banking sector representatives	Exploratory interview	15 November 2016	No
2	Two banking sector representatives	Exploratory interview	19 December 2016	No
3	FIU employee	Semi-structured interview	14 June 2017	No
4	Banking sector representative	Conversation	9 October 2017	No
5	FIU employee	Semi-structured interview	26 December 2017	No
6	FIU employee	Semi-structured interview	5 March 2018	No
7	Former head of FIU	Semi-structured interview	31 May 2018	Yes
8	Two FIU employees	Exploratory interview	6 June 2018	No
9	Former head of FIU	Semi-structured interview	6 September 2018	Yes
10	Consultant on NGO/NPO regulation	Semi-structured interview	7 September 2018	Yes
11	FIU employee	Semi-structured interview	14 September 2018	Yes
12	Europol employee	Semi-structured interview	1 October 2018	Yes
13	Financial crime consultant	Semi-structured interview	16 October 2018	Yes
14	Intelligence analyst (government)	Unstructured interview	19 October 2018	No
15	Europol employee	Semi-structured interview	5 December 2018	Yes
16	FIU employee	Semi-structured interview	6 December 2018	Yes
17	FIU employee	Semi-structured interview	8 January 2019	Yes
18	FIU employee	Semi-structured interview	17 January 2019	Yes
19	Police officer countering terrorism	Semi-structured interview	31 January 2019	No
20	Two police officers countering terrorism	Unstructured interview	1 February 2019	No
21	FIU employee	Semi-structured interview	26 January 2019	Yes
22	FIOD employee	Semi-structured interview	10 May 2019	Yes
23	Three employees of European Commission	Semi-structured interview	16 May 2019	Yes
24	Three employees of intergovernmental organization	Exploratory conversation	5 July 2019	No
25	Head of FIU	Semi-structured interview	13 August 2019	Yes
26	Head of International cooperation department of an FIU	Semi-structured interview	6 February 2020	Yes
27	Head of International cooperation department of an FIU	Semi-structured interview	26 February 2020	Yes
28	FIU employee	Structured Questionnaire	12 March 2020	No
29	FIU employee	Structured Questionnaire	5 May 2020	No

Summary

In the wake of the wars on drugs and terror, countries around the globe have established Financial Intelligence Units – often abbreviated simply as FIUs – to analyze financial transactions for security purposes. FIUs are a relatively new type of public organization that provides intelligence in the context of combatting money laundering and terrorism financing. Because financial transactions flow irrespective of national borders, FIUs are bound to join forces, coordinate their operations, and exchange their expertise and financial intelligence. However, FIUs are diverse organizations that operate in varied political, cultural, and economic environments with different legal regulations concerning privacy, data handling, and human rights. This dissertation examines how this collective of diverse security organizations overcomes geographical distance and works across operational difference, in order to follow illicit finance across borders. How do FIUs coordinate their operations transnationally and exchange financial intelligence across geographical distance and organizational difference?

Drawing on literatures at the intersection of science and technology studies (STS) and international relations (IR), the dissertation adopts four 'vantage points' to obtain a view of how transnational processes are coordinated in practice, where political negotiation and the reconfiguration of power relations take place. The vantage points are *FIU-the Netherlands*, where the financial intelligence that is exchanged is produced; the *EU FIUs Platform*, a European Commission Expert Group that discusses how cross-border tracking practices are organized; the *numbering practices* of FIUs, through which FIUs coordinate cross-border operations; and *circuits of trust*, informal relationships that make the sharing of financial intelligence possible. The dissertation concludes that it is the relatively informal nature of international agreements in combination with FIU operational autonomy that enables FIUs to overcome distance and difference and share privacy-sensitive intelligence. This conclusion raises questions of accountability, oversight, and proportionality in FIU operations.

The dissertation is presented in seven chapters. **Chapter 1** introduces the context of FIU operations, the research questions, and the theoretical framework. The question of how to study transnational or global processes in daily practice has received considerable attention in a diversity of disciplines, such as STS, IR, and what can be roughly understood as the anthropology of globalization. Speaking to these literatures, this dissertation's conceptual approach contributes to the study of transnational or global processes in practice, by making three analytical moves. First, it moves from studying cooperation to studying *co-ordination*, in order to account for the coexistence of different realities of financial intelligence, how these entangle, and how they are

continuously reordered and reassembled across geographies. Second, it places particular emphasis on the *materiality* of transnational processes, including the role of non-human actors, such as software programs, meeting rooms, and numbering practices. Third, it proposes to study *vantage points*. That is, each empirical chapter chooses a particular advantageous point to understand practices through which transnational processes are coordinated and where political negotiations and the reconfiguration of power relations take place.

Chapter 2 discusses the methodology of the dissertation, presenting the ways in which the data were collected and the conduct of the qualitative research regarding the *practices* of FIUs. The thesis inquires into the daily operations of FIUs and the experiences of practitioners; their challenges, dilemmas, negotiations, conflicts, and political stakes. In order to gain access to the secretive security field of financial intelligence, in which many processes and aspects – such as the actual financial transactions – are classified as secret and not accessible to researchers, a flexible and iterative research design was applied. The fieldwork was conducted between 2016 and 2020, and employed methods such as semi-structured interviews with FIU professionals and other security practitioners; participant observation at practitioner conferences, workshops, and trainings; and document analysis of policy reports, meeting minutes, and legislation. The research, furthermore, applied the grounded theory approach, constantly switching back and forth between empirics and theory, gradually selecting the most promising vantage points, and sharpening the research focus, questions, and conclusions.

Chapter 3 adopts *FIU-the Netherlands* as its vantage point. To understand how FIUs work across distance and difference, this first vantage point is key because it provides a perspective on how the actual financial intelligence that is exchanged between FIUs is produced in practice. The chapter focuses on the three core activities that all FIUs undertake: *collecting* transaction information from commercial organizations such as banks, *analyzing* this information within the FIU, and *disseminating* intelligence to law enforcement, judiciary, and foreign FIUs. Little is known about these internal processes because the analysis of transaction information is shrouded in secrecy. In order to analyze FIU operations despite the secrecy that is part and parcel of the sector, the chapter uses novel methods to 'encircle' the secrecy, focusing not on the kernel of the secret but on the mundane practices of FIUs surrounding it. The chapter concludes by raising questions regarding privacy, proportionality, and accountability. These are further discussed in Chapter 6 and in the thesis conclusion.

Chapter 4 adopts the *EU FIUs Platform* as its vantage point. Within the platform, representatives from 30 European FIUs coordinate cross-border operations and discuss the exchange of expertise and financial intelligence. From this vantage point it becomes possible to view how geographically dispersed security actors produce shared understandings of financial intelligence. Different ways of constructing financial

intelligence encounter each other, transcending different understandings of security threats, different legal and institutional frameworks, and different ways in which FIUs operate and share financial intelligence across borders. In particular, the chapter traces the phrase 'for intelligence purposes', which is often added as a clause by FIUs to the intelligence they share. The chapter demonstrates the *interpretive flexibility* of this phrase, as it enables actors to work together across heterogeneous understandings, and its *flexible scalability*, in that it makes it possible for practitioners to assign and navigate several scales at the same time. The chapter concludes that to enable the transnational circulation of financial intelligence in practice, seemingly trivial elements, such as this phrase, are crucial.

Chapter 5 adopts as its vantage point the *numbering practices* of FIUs. Increasingly, FIUs gather data – in particular, numbers and statistics – on security threats, such as money laundering and terrorist financing. FIUs gather these data in different ways, through different practices of categorizing, measuring, and standardizing XML formats, and by the use of different software systems. However, despite the different standardizations and the lack of harmonization, the production of numbers and statistics is highly valued by security practitioners around the globe. The numbering practices they use, this chapter shows, serve to provide a technical, depoliticized and technocratic vocabulary that enables FIUs to encounter each other across distance and difference. Without touching on politically sensitive issues, such as what terrorism or terrorist financing actually entails, statistics and numbering practices provide words, concepts, and methods that can be debated, agreed upon, and used to settle disputes. The numbering practices make it possible to develop a transnational space that can be governed, while the urgency of security threats, such as terrorist financing, provides the legitimacy for the sharing of intelligence.

Chapter 6 adopts *circuits of trust* as its vantage point. Practitioners meet and generate trust through a circuit of events, conferences, workshops, seminars, and webinars. This geographically dispersed circuit yields key insights regarding the political and geopolitical exchange of financial intelligence, by which informal political practices and circuits of trust make sensitive financial data and transactions internationally shareable. The chapter examines three practices to understand the importance of trust: the use of trust circuits to navigate a transnational 'legal grey zone'; the use of trust to make intelligence sharing possible (or impossible); and the implicit notions of trustworthiness and untrustworthiness at work in the circuit, which lead to inclusion or exclusion. The chapter reflects, in conclusion, on the decision-making powers and autonomy of FIUs, especially with regard to accountability and public oversight. This topic is returned to in the final chapter of the dissertation.

Chapter 7, in conclusion, returns to the main research question and connects the different vantage points adopted in the empirical chapters. The conclusion distills two possible areas for further research: to unpack the question of how FIU intelligence

is used further down the chain of financial security and to study the increasingly important role of non-Western FIUs. The main conclusion of this chapter is that it is the relatively informal nature of international agreements in combination with the autonomy of FIU operations that enables FIUs – through hard (coordinating) work – to share privacy-sensitive intelligence around the globe. The chapter raises questions about the societal consequences of financial intelligence and the operations of FIUs, concerning proportionality, oversight, and accountability. These will be of interest not only to academics but as well to politicians, policymakers, and practitioners.

Samenvatting

In de nasleep van de oorlogen tegen drugs en terreur hebben landen over de hele wereld Financial Intelligence Units opgericht – vaak eenvoudigweg afgekort als FIU's – om financiële transacties te analyseren voor veiligheidsdoeleinden. FIU's zijn een relatief nieuw type publieke organisatie die inlichtingen levert in het kader van de bestrijding van witwassen en terrorismefinanciering. Omdat financiële transacties gemakkelijk over landsgrenzen heen plaatsvinden, zijn FIU's genoodzaakt om hun krachten te bundelen, hun operaties te coördineren en hun expertise en financiële inlichtingen uit te wisselen. FIU's zijn echter diverse organisaties, die opereren in verschillende politieke, culturele en economische situaties met verschillende regelgeving op het gebied van privacy, gegevensverwerking en mensenrechten. Dit proefschrift onderzoekt hoe dit collectief van diverse veiligheidsorganisaties samenwerkt over geografische afstand, en operationele verschillen overbrugt om verdachte geldstromen te volgen en te bestrijden. Hoe coördineren FIU's hun transnationale operaties en wisselen ze financiële informatie uit over geografische afstanden, en hoe gaan ze om met organisatorische verschillen?

Voortbouwend op literatuur op het snijvlak van Science and Technology Studies (STS) en internationale betrekkingen (IR), hanteert het proefschrift vier 'uitkijkpunten' om een beeld te krijgen van hoe transnationale processen in de praktijk worden gecoördineerd. Deze uitkijkpunten maken de politieke onderhandelingen en de herconfiguratie van machtsrelaties inzichtelijk. De uitkijkpunten die gehanteerd worden zijn *FIU-Nederland*, waar de inlichtingen die internationaal worden uitgewisseld worden geproduceerd; het *EU FIUs Platform*, een deskundigengroep van de Europese Commissie die bepaalt hoe grensoverschrijdende activiteiten worden georganiseerd; de *nummeringspraktijken* van FIU's, door middel waarvan FIU's grensoverschrijdende operaties kunnen coördineren; en de *vertrouwenscircuits*, de informele relaties die het delen van financiële informatie mogelijk maken. Het proefschrift concludeert dat het relatief informele karakter van internationale overeenkomsten in combinatie met de operationele autonomie van FIU's, maakt dat FIU's in staat zijn om afstand en verschil te overbruggen en privacygevoelige informatie te delen. Deze conclusie roept vragen op over de proportionaliteit en verantwoording van, en de toezicht op FIU-operaties.

Het proefschrift bestaat uit zeven hoofdstukken. **Hoofdstuk 1** introduceert de context van FIU-operaties, de onderzoeksvragen en het theoretisch kader van het onderzoek. De vraag hoe transnationale of globale processen in de dagelijkse praktijk bestudeerd kunnen worden, heeft veel aandacht gekregen vanuit een diversiteit aan disciplines, zoals STS, IR, en wat grofweg kan worden samengebracht als de antropologie van globalisering. Voortbouwend op deze literatuur, draagt de conceptuele benadering

van dit proefschrift bij aan de studie van transnationale of globale processen in de praktijk, door drie analytische bewegingen te maken. Ten eerste richt dit onderzoek zich niet op de samenwerking maar de *coördinatie* tussen FIU's. Op deze manier is er aandacht voor hoe verschillende realiteiten van financiële inlichtingen naast elkaar bestaan, hoe deze met elkaar verstrengeld zijn en hoe ze voortdurend opnieuw worden samengesteld in verschillende geografische gebieden. Ten tweede legt het proefschrift bijzondere nadruk op de *materialiteit* van transnationale processen, inclusief de rol van niet-menselijke actoren, zoals softwareprogramma's, vergaderruimten en nummeringspraktijken. Ten derde hanteert het proefschrift verschillende *uitkijkpunten*. Dat wil zeggen, elk empirisch hoofdstuk hanteert een gunstig punt van analyse dat zicht biedt op praktijken waar transnationale processen worden gecoördineerd en waar politieke onderhandelingen en de herconfiguratie van machtsverhoudingen plaatsvindt.

Hoofdstuk 2 bespreekt de methodologie van het proefschrift, presenteert de manieren waarop de gegevens zijn verzameld en bespreekt de uitvoering van het kwalitatieve onderzoek naar de *praktijken* van FIU's. Het proefschrift onderzoekt de dagelijkse praktijk van FIU's en de ervaringen van mensen: hun uitdagingen, dilemma's, onderhandelingen, conflicten en politieke belangen. Om toegang te krijgen tot het relatief geheime veld van de financiële inlichtingen, waarin veel processen en financiële aspecten – zoals de daadwerkelijke financiële transacties – als geheim zijn geclassificeerd en niet toegankelijk zijn voor onderzoekers, is een flexibel en iteratieve onderzoeksbenadering toegepast. Het veldwerk werd uitgevoerd tussen 2016 en 2020 en maakte gebruik van methoden zoals semigestructureerde interviews met FIU-medewerkers en andere veiligheidsprofessionals; participerende observatie bij praktijkconferenties, workshops en trainingen; en documentanalyse van beleidsrapporten, notulen van vergaderingen en wetgeving. Het onderzoek paste bovendien de *Grounded Theory* benadering toe, waarbij er een voortdurende wisselwerking plaatsvindt tussen empirie en theorie, om geleidelijk de meest veelbelovende gezichtspunten te selecteren en de onderzoeksfocus, vragen en conclusies continu aan te scherpen.

Hoofdstuk 3 hanteert de *FIU-Nederland* als uitkijkpunt. Om te begrijpen hoe FIU's over afstand en verschil werken, is dit eerste gezichtspunt van cruciaal belang omdat het een perspectief biedt op hoe de daadwerkelijke financiële inlichtingen die tussen FIU's worden uitgewisseld, in de praktijk tot stand komen. Het hoofdstuk richt zich op de drie kernactiviteiten die FIU's ondernemen: het *verzamelen* van transactie-informatie van commerciële organisaties zoals banken, het *analyseren* van deze informatie binnen de FIU en het *verspreiden* van inlichtingen naar rechtshandhaving, justitie en buitenlandse FIU's. Over deze interne processen is weinig bekend omdat de analyse van transactie-informatie geheime processen betreft. Het hoofdstuk gebruikt nieuwe methoden om de geheimhouding te 'omcirkelen', waarbij de focus niet ligt op de kern van het geheim, maar op de alledaagse praktijken van FIU's eromheen. Het hoofdstuk wordt afgesloten met vragen over privacy, proportionaliteit en verantwoording. Deze

worden verder besproken in Hoofdstuk 6 en in de conclusie van het proefschrift.

Hoofdstuk 4 hanteert het *EU FIU's Platform* als uitkijkpunt. Binnen het platform coördineren vertegenwoordigers van dertig Europese FIU's grensoverschrijdende operaties en bespreken ze de uitwisseling van expertise en financiële inlichtingen. Vanuit dit punt wordt het mogelijk om te zien hoe geografisch verspreide veiligheidsactoren tot gedeelde inzichten komen. Verschillende benaderingen van het produceren van financiële inlichtingen komen hier samen, waarbij verschillende opvattingen over veiligheidsdreigingen en verschillende wettelijke en institutionele kaders waarbinnen FIU's opereren ter sprake komen. Het hoofdstuk traceert met name de zinsnede 'voor inlichtingendoeleinden', die door FIU's vaak als clausule wordt toegevoegd aan de inlichtingen die zij delen. Het hoofdstuk demonstreert de *interpretatieve flexibiliteit* van deze clausule, omdat het actoren in staat stelt om samen te werken over heterogene begrippen heen. Het hoofdstuk demonstreert ook de *flexibele schaalbaarheid* van de clausule, door te laten zien hoe deze clausule actoren in staat stelt om verschillende schaalgroottes tegelijkertijd te navigeren. Het hoofdstuk concludeert dat om de transnationale verspreiding van financiële inlichtingen in de praktijk mogelijk te maken, ogenschijnlijk triviale elementen, zoals deze clausule, cruciaal zijn.

Hoofdstuk 5 neemt de *nummeringspraktijken* van FIU's als uitkijkpunt. FIU's verzamelen steeds vaker gegevens – met name cijfers en statistieken – over veiligheidsdreigingen, zoals witwassen en terrorismefinanciering. FIU's verzamelen deze gegevens op verschillende manieren, door verschillende methoden van categoriseren, meten en standaardiseren van XML-formaten te gebruiken, en door het gebruik van verschillende softwaresystemen. Ondanks de verschillende standaardisaties en het gebrek aan harmonisatie, wordt de productie van cijfers en statistieken echter zeer gewaardeerd door veiligheidsactoren over de hele wereld. De nummeringspraktijken die ze gebruiken, zo laat dit hoofdstuk zien, verschaffen een technisch, gedepolitiseerd en technocratisch vocabulaire dat FIU's in staat stelt om elkaar over afstand en verschil te verbinden. Zonder in te gaan op politiek gevoelige kwesties, zoals wat terrorisme of terrorismefinanciering eigenlijk inhoudt, bieden statistieken en nummeringspraktijken de woorden, concepten en methoden waarover kan worden gedebatteerd, overeenstemming kan worden bereikt of geschillen kunnen worden beslecht. De nummeringspraktijken maken het mogelijk om een transnationale ruimte te ontwikkelen die kan worden bestuurd, terwijl de urgentie van veiligheidsdreigingen, zoals terrorismefinanciering, de legitimiteit biedt voor het delen van inlichtingen.

Hoofdstuk 6 neemt *vertrouwenscircuits* als uitkijkpunt. Professionals ontmoeten elkaar en ontwikkelen vertrouwen via een circuit van evenementen, conferenties, workshops, seminars en webinars. Dit geografisch verspreide circuit levert belangrijke inzichten op over de politieke en geopolitieke uitwisseling van financiële inlichtingen. Het hoofdstuk onderzoekt drie praktijken om het belang van vertrouwen te begrijpen: het gebruik van vertrouwenscircuits om transnationale

'juridische grijze zones' te navigeren; het gebruik van vertrouwen om het delen van inlichtingen (on)mogelijk te maken; en het hoofdstuk onderzoekt hoe impliciete noties van betrouwbaarheid en onbetrouwbaarheid leiden tot in- of uitsluiting. In het hoofdstuk wordt tot slot gereflecteerd op de beslissingsbevoegdheid en autonomie van FIU's, met name op het gebied van verantwoording en publiek toezicht. Dit onderwerp komt terug in het laatste hoofdstuk van het proefschrift.

Hoofdstuk 7, tot slot, keert terug naar de hoofdvraag van het onderzoek en verbindt de verschillende uitkijkpunten die in de empirische hoofdstukken zijn gehanteerd. De conclusie identificeert twee mogelijke gebieden voor verder onderzoek: het ontrafelen van de vraag hoe FIU-inlichtingen verderop in de keten van financiële opsporing worden gebruikt; en het bestuderen van de steeds belangrijkere rol van niet-westerse FIU's. De belangrijkste conclusie van het proefschrift is dat het relatief informele karakter van internationale afspraken in combinatie met de autonomie van FIU's, hen in staat stelt om privacygevoelige informatie wereldwijd te delen. Deze conclusie roept vragen op over de maatschappelijke gevolgen van financiële inlichtingen en het optreden van FIU's op het gebied van proportionaliteit, toezicht en verantwoording. Deze vragen zijn niet alleen interessant voor academici, maar ook voor politici, professionals en beleidsmakers.

Acknowledgements

This dissertation could not have been written without the help of my supervisors, colleagues, family, and friends. It is the product of an academic inquiry that started when I began my bachelor in anthropology 14 years ago, in 2009. I remember how free I felt when discovering that at the University of Amsterdam knowledge is not only produced, but also questioned. It was a pleasure to study at the Spinhuis, where the anthropologists and sociologists resided at the time. It seemed that the more I learned, the less I actually knew. What followed was a more than decade-long exploration of the tools that the social sciences have to offer. In that exploration I was accompanied by many others, both within and outside the university. This dissertation is not the end of that pursuit. It is, however, a good opportunity to take stock and express my gratitude to all those who have been so important in its co-production.

First, I thank my promotor Marieke de Goede, who was part of the exploration for most of this decade. You have been a very stimulating and motivating supervisor, providing space for creativity and free thinking, yet also knowing when to urge me to keep a firm focus. I thank my daily co-promotor, Rocco Bellanova, for his multifarious guidance: theoretically when discussing STS, methodologically during fieldtrips, and also concerning practical things such as a cover letter. You have been a supervisor pur sang. Another important part of my exploration was my late supervisor, Mario Rutten. He introduced me to ethnography and shared with me his passion for the social sciences.

This dissertation is part of the FOLLOW research project. It was an intellectual pleasure to work in this group, and see it develop and progress from 2016 to 2022. I thank all those who in different capacities were involved in this project: Anthony Amicelle, Asma Balfaqih, Andreas Baur, Malcolm Campbell-Verduyn, Maja Dehouck, Marijn Hoijtink, Moritz Hütten, Marie Irmer, Beste İşleyen, Bruno Magalhães, Lilly Pijnenburg Muller, Anneroos Planqué-van Hardeveld, Jasper van der Kist (my paranymph!), Polly Pallister-Wilkins, Natalie Welfens, Mara Wesseling and Carola Westermeier. I extend special thanks to my fellow PhDs Tasniem Anwar and Esmé Bosma. It was a pleasure working with you and organizing and visiting events together.

I thank the other PhDs of the AISSR as well, particularly my colleagues in room B9.01 and our neighboring rooms. It is a shame that, just when many of us had finished our fieldwork and were in the writing phase, Covid-19 forced us all to our desks at home. I thank Astrid, Barbara, Bart, Becky, Chris, Daniel, Danny, David, Dawid, Dilliara, Douwe, Edward, Javier, Jessica, Joan, Joep, Jos, Joshua, Kris, Merel, Milan, Mira, Nilma, and Roberto. I also thank the many other colleagues who were part of the AISSR and I had the pleasure to meet over the years – too many to mention! I'd also

like to express my appreciation for the Amsterdam Institute for Social Science Research (AISSR) itself and the program group Transnational Configurations, Conflict and Governance. Finally, I thank my current colleagues at the PPLE college, where I keep meeting new and interesting academics from the social sciences writ large.

My friends and family were very important in keeping me from getting lost in the frenzied and occasionally detached world of the social sciences. I thank friends from different parts of my life: my old friends, many of whom have gathered again in the WhatsApp group "Overveen Crew [Censored]", my friends from university such as the "Spice Girls", my old living community SOUS and the FHS, the Montelbaners, and many other friends, such as the Keesmaat/Van der Veldt, De Beer, and Zoetemeijer/Van Walsem families.

This dissertation is dedicated to my – in anthropological terms – nuclear family or kerngezin. I thank my parents for their support – which sounds cliché, but their support has been a cornerstone of my life and of this dissertation. I thank my brother Guus for all the fun we always have, and for designing the wonderful cover of this book. I also thank my late uncle Bart, who sadly could not see this PhD finished, as well as Michèle, Lucas, Nathalie, Daan and Huub. I thank Willem and Jolanda, Dirk y Nuria, Willem og Nathali og Elliot, Annemieke, and Cornelieke und Ursel. I thank my in laws, the Bosmas, and particularly Matty and Jáda. Finally, I thank Esmé, who transferred from the FOLLOW project to my nuclear family: the most wonderful result of this PhD I could have wished for!

Pieter Lagerwaard
Amsterdam, February 2023

In the wake of the wars on drugs and terror, countries around the globe have established Financial Intelligence Units – often abbreviated simply FIUs – that analyze financial transactions for security purposes. FIUs are relatively new public organizations that provide intelligence in the context of combatting money laundering and terrorist financing. Because financial transactions flow irrespective of national borders, FIUs are bound to join forces, coordinate their operations, and exchange their expertise and intelligence. However, FIUs are diverse organizations, that operate in varied political, cultural, and economic environments, with different legal regulations concerning privacy, data handling, and human rights. This dissertation examines how this collective of diverse security organizations overcomes geographical distance and works across operational difference, in order to follow illicit finance across borders. How do FIUs coordinate their operations transnationally and exchange financial intelligence across geographical distance and organizational difference?

Drawing on literatures at the intersection of Science and Technology Studies (STS) and International Relations (IR), the dissertation adopts four 'vantage points' to analyze the coordination of transitional processes in practice, where political negotiation and the reconfiguration of power relations take place. The vantage points are the FIU-the Netherlands, where the financial intelligence that is exchanged is produced; the EU-FIU Platform, an EU Commission expert group that discusses how cross-border tracking practices are organized; the numbering practices of FIUs, through which FIUs coordinate cross-border operations; and circuits of trust, that is, informal relationships that make the sharing of financial intelligence possible. The dissertation concludes that it is the relatively informal nature of international agreements in combination with FIU operational autonomy that enables FIUs to overcome distance and difference and share privacy-sensitive intelligence. This conclusion raises questions of accountability, oversight, and proportionality of FIU operations. These will be of interest not only to academics, but to politicians, policymakers, and practitioners as well.