Banks as security actors

Countering terrorist financing at the human-technology interface

Bosma, E.

Publication date
2022

Summary

Banks have become private security actors. As "gatekeepers" of the financial system, they are legally obliged to conduct customer research and monitor bank accounts for unusual or suspicious transactions. If they identify transactions with potential links to money laundering or terrorist financing, they must report these to their national Financial Intelligence Unit (FIU). Because of the sheer volume of financial transactions that banks process daily, detection of financial crime relies on digital security technologies that help analysts categorise and identify risky customers and financial transactions. This thesis analyses how banks practice counter-terrorist financing (CTF) and how they experiment with technologies to make authoritative security decisions.

Contributing to theories at the intersection of Science and Technology Studies (STS) and International Relations (IR), the thesis develops a dynamic and processual understanding of risk detection and of processes of financial inclusion and exclusion. The research is based on fieldwork observations in the financial crime sector in the Netherlands and the United Kingdom. It includes three months' observation at a major Dutch bank, alongside interviews with public and private actors and document analysis. This dissertation analyses security at the human-technology interface, specifically during the production of customer risk profiles, in the design and use of transaction monitoring systems and in the emergence of public-private partnerships to counter terrorist financing. The research concludes that there is a misalignment between regulation and practice: the implementation of CTF rules does not lead to the effective prevention of terrorist financing in practice.

This thesis encompasses seven chapters. The first three introduce the research and outline the theory and methods used. Chapters 4-6 present the empirical work, analysing how banks practice CTF and how they experiment with technologies to make authoritative security decisions. The first two empirical chapters focus on two traditional, and regulated, tasks of banks: "know your customer" (KYC) practices (Chapter 4) and automated transaction monitoring systems (Chapter 5). The third empirical chapter (Chapter 6) traces the emergence of public-private partnerships that have arisen in reaction and as a solution to the challenges in traditional financial crime detection. Chapter 7, the conclusion, recaps and connects the chapters.

Chapter 1 traces how banks have become gatekeepers of the financial system and discusses the thesis' aims, relevance, research questions and approach. The chapter sets out how the Anti-Money-Laundering and Counter-Terrorist Financing framework of the European Union and other obligations imposed on banks have reshaped banks'

traditional role as intermediaries into a new role as a private security actor. Furthermore, the chapter situates the practice-oriented approach of the thesis at the intersection of STS and IR and demonstrates how the ethnographic nature of the current research, its foregrounding of materials and technologies, and its documentation of novel public-private partnerships contribute to the existing literature. Finally, the chapter presents the research questions and offers an outline of the remainder of the thesis.

Chapter 2 develops the theoretical framework of the research. Based on work at the intersection of STS and IR, particularly Akrich's work, it outlines a *de-scriptive* approach to study *experimentation* with security in practice. This de-scriptive approach is three-fold. First, it explores why a focus on the interpretation and application of rules in practice is crucial to amplify the experimental nature of risk-based security practices such as in CTF. Second, building on Actor-Network Theory (ANT), the notion of de-scription is advanced to conceptualise and operationalise the role of materials and digital security technologies as important mediators of CTF in practice. Third, these de-scriptive approaches are argued as useful for purposes of transparency and accountability, in the sense that they expose how and where political choices are (not) inscribed into technologies. The de-scriptive approach, in sum, helps to draw out how technologies enable and constrain security in practice.

Chapter 3 outlines the qualitative methods deployed in this research. To understand the daily dilemmas banks face in countering terrorist financing, the work builds on ethnographic study at multiple sites. The first part of the chapter addresses the challenge posed by secrecy when doing ethnographies of technologies. The second part provides insight into my practice of studying the bank. It zooms in particularly on how I gained access to the bank, methods of data collection and data analysis. The third part elaborates on the methodological strategies used, as these may be useful to other researchers in the security field. Based on insights from STS, I advance the concept of *sites of experimentation* to refer to sites where digital security technologies can be observed, and I discuss two methodological starting points: (i) following digital security technologies from design to use and (ii) observation of human-computer interaction. Lastly, the chapter briefly discusses the validation and limitations of the research.

Chapter 4 analyses how customer risk profiles are produced, with which customers are labelled as "acceptable" or "unacceptable", throughout what banks term "the client lifecycle". This cycle encompasses screening and monitoring techniques deployed from the moment a customer is "onboarded", to the ongoing client and transaction monitoring process, as well as the potential "offboarding", or termination of the bank's relationship with a client. This dynamic process includes risk assessments, watchlist screening, transaction monitoring and manual research into high-risk clients. The findings suggest that the processual production of a customer risk profile is increasingly reliant on public sources and on the data underpinning digital security technologies.

The chapter, furthermore, demonstrates the increased relevance of "know your data" in KYC practices, particularly with regard to issues of data quality, the temporality of data and data-related liabilities. It concludes that the origins of security decisions lie in early processes of data organisation and in the way digital technologies are designed and used.

Chapter 5 deploys Akrich's notion of *de-scription* to explore how banks experiment with automated transaction monitoring systems in an attempt to detect terrorist financing. First, the chapter analyses the challenge of finding workable "input" for transaction monitoring systems, in the form of indicators of terrorist financing. Banks experiment with the formulation of these indicators and with the *tuning* of settings in their transaction monitoring systems. The second part discusses the design and use of these systems via three "scripts": rules-based transaction monitoring, supervised machine learning models and unsupervised machine learning models. The aim of all these systems is the detection of transactions with a potential link to terrorist financing for reporting to FIUs. However, the scripts are also found to present privacy and ethical dilemmas to analysts at banks. Moreover, the analysis suggests that automated transaction monitoring systems may in practice be ineffective in detecting terrorist financing threats.

Chapter 6 examines financial intelligence sharing for CTF purposes enabled via public-private partnerships. The chapter thus moves beyond the focus on traditional forms of CTF to discuss experimentation with targeted intelligence sharing in public-private partnerships. Two such partnerships are traced: one in the United Kingdom (JMLIT) and one in the Netherlands (the TF Taskforce). Public-private partnerships facilitate law enforcement's sharing of tactical information with banks outside the purview of official criminal investigations, in a bid to more effectively detect terrorist financing. In documenting the quest for an adequate legal basis for such collaborations, the chapter suggests that *rule following* around CTF is shaped by creative interpretation, experimentation and reappropriation of existing rules. Indeed, this process appears to have accelerated the formulation of new rules. I coin the concept *techno-legal gateway* to refer to the way the combination of technological infrastructure and legal interpretation has enabled novel forms of *targeted* as well as *networked* intelligence sharing.

Chapter 7 presents the research conclusions. It recaps the main findings of the research, explores the core theoretical contributions of the dissertation, identifies societal implications and offers suggestions for future research. The chapter considers the enormous deployment of human and financial resources and the extent to which this contributes to fighting financial crime, and concludes that the current system is ineffective and inefficient. There is an evident misalignment between the *regulations* that oblige banks to detect and prevent terrorist financing and the *practice* of countering terrorist financing in banks. The analysis of human-technology interactions and of the data underlying security technologies demonstrates that it is extremely difficult for banks to discover in financial transaction patterns the *intention* to finance terrorism

and subsequently *prevent* it from happening. The chapter takes into account the societal implications that emerge, such as the general privacy impact of large-scale financial surveillance, including the risk of ethnic or religious profiling, the unintended consequences such as de-risking and financial exclusion, and the blurring of accountability in increasingly digitised security contexts. It is important to consider to what purposes the counter-terrorist finance toolbox is created and whether these goals are achieved. Ultimately, the question of what role private actors should play in far-reaching security decisions is a political one.

Samenvatting

Banken zijn particuliere veiligheidsactoren geworden. Als "poortwachters" van het financiële systeem, zijn zij wettelijk verplicht cliëntenonderzoek te verrichten en bankrekeningen te monitoren op ongebruikelijke of verdachte transacties. Als zij transacties ontdekken die mogelijk verband houden met het witwassen van geld of de financiering van terrorisme, moeten zij deze melden aan hun nationale *Financial Intelligence Unit* (FIU). Vanwege de enorme hoeveelheid financiële transacties die banken dagelijks verwerken, is de opsporing van financiële criminaliteit afhankelijk van digitale veiligheidstechnologieën die analisten gebruiken voor het categoriseren en identificeren van risicovolle klanten en financiële transacties. Deze dissertatie analyseert hoe banken terrorismefinanciering bestrijden in de praktijk en hoe zij experimenteren met technologieën om gezaghebbende beslissingen te nemen.

De dissertatie draagt bij aan theorieën op het snijvlak van *Science and Technology Studies* (STS) en Internationale Betrekkingen (IB) en ontwikkelt een dynamisch en procesmatig begrip van risicodetectie en van processen van financiële in- en uitsluiting. Het onderzoek is gebaseerd op veldwerkobservaties in de financiële criminaliteitssector in Nederland en het Verenigd Koninkrijk. Het omvat drie maanden observatie bij een grote Nederlandse bank, interviews met publieke en private actoren en documentanalyse. Het proefschrift analyseert de veiligheid op het raakvlak tussen mens en technologie, specifiek bij het opstellen van klantrisicoprofielen, het design en gebruik van transactiemonitoringsystemen en bij het ontstaan van publiek-private samenwerkingsverbanden om terrorismefinanciering tegen te gaan. Het onderzoek concludeert dat er sprake is van een scheve verhouding tussen regelgeving en praktijk: de implementatie van regels die terrorismefinanciering dienen te bestrijden leidt in de praktijk niet tot effectieve preventie van terrorismefinanciering.

Dit proefschrift bestaat uit zeven hoofdstukken. De eerste drie introduceren het onderzoek en schetsen de gebruikte theorie en methoden. In de hoofdstukken 4 tot en met 6 wordt het empirische werk gepresenteerd, waarbij geanalyseerd wordt hoe banken de bestrijding van terrorismefinanciering in de praktijk brengen en hoe zij experimenteren met technologieën om gezaghebbende veiligheidsbeslissingen te nemen. De eerste twee empirische hoofdstukken richten zich op twee traditionele, en gereguleerde, taken van banken*: "know your customer"* (KYC) praktijken (hoofdstuk 4) en geautomatiseerde transactiemonitoringsystemen (hoofdstuk 5). Het derde empirische hoofdstuk (hoofdstuk 6) schetst de opkomst van publiek-private partnerschappen die zijn ontstaan als reactie op en als oplossing voor de uitdagingen in de traditionele opsporing

van financiële criminaliteit. In hoofdstuk 7, de conclusie, worden de hoofdstukken samengevat en met elkaar verbonden.

Hoofdstuk 1 beschrijft hoe banken poortwachters van het financiële systeem zijn geworden en bespreekt de doelen, relevantie, onderzoeksvragen en aanpak van het proefschrift. In dit hoofdstuk wordt uiteengezet hoe het anti-witwas- en anti-terrorismefinancieringskader van de Europese Unie en de verplichtingen die aan banken worden opgelegd de traditionele rol van banken als intermediair hebben veranderd in een nieuwe rol als private veiligheidsactor. Verder situeert het hoofdstuk de praktijkgerichte benadering van het proefschrift op het snijvlak van STS en IB en toont het aan hoe de etnografische aard van het huidige onderzoek, de nadruk op materialiteit en technologieën, en de documentatie van nieuwe publiek-private samenwerkingsverbanden bijdragen tot de bestaande literatuur. Ten slotte presenteert het hoofdstuk de onderzoeksvragen en geeft het een overzicht van het proefschrift.

Hoofdstuk 2 ontwikkelt het theoretisch kader van het onderzoek. Gebaseerd op werk op het snijvlak van STS en IB, met name het werk van Akrich, schetst het een "de-scriptieve" benadering om veiligheidsexperimenten in de praktijk te bestuderen. Deze de-scriptieve benadering is drieledig. Ten eerste wordt onderzocht waarom een focus op de interpretatie en toepassing van regels in de praktijk cruciaal is om het experimentele karakter van risicogebaseerde veiligheidspraktijken, zoals de bestrijding van terrorismefinanciering, te versterken. Ten tweede wordt, voortbouwend op de actor-netwerktheorie, de notie van de-scriptie ontwikkeld om de rol van materialen en digitale beveiligingstechnologieën als belangrijke *mediators* van de bestrijding van terrorismefinanciering in de praktijk te conceptualiseren en te operationaliseren. Ten derde wordt gesteld dat deze de-scriptieve benaderingen nuttig zijn met het oog op transparantie en verantwoordingsplicht, in die zin dat ze blootleggen of, hoe en waar politieke keuzes in technologieën zijn verankerd. De de-scriptieve benadering helpt, kortom, om duidelijk te maken hoe technologieën in de praktijk bepaalde veiligheidspraktijken accommoderen, of juist verhinderen.

Hoofdstuk 3 geeft een overzicht van de kwalitatieve methoden die in dit onderzoek zijn gebruikt. Om inzicht te krijgen in de dagelijkse dilemma's waarmee banken worden geconfronteerd bij het tegengaan van terrorismefinanciering, is het werk gebaseerd op etnografisch onderzoek op meerdere locaties. Het eerste deel van het hoofdstuk gaat in op de uitdaging die geheimhouding vormt voor een etnografie van technologieën. Het tweede deel geeft inzicht in de praktijk van het bestuderen van een bank. Er wordt met name ingezoomd op de manier waarop ik toegang kreeg tot de bank, de methoden van dataverzameling en data-analyse. Het derde deel gaat dieper in op de gebruikte methodologische strategieën, aangezien deze nuttig kunnen zijn voor andere onderzoekers van veiligheidsvraagstukken. Op basis van inzichten uit STS ontwikkel ik het concept *sites of experimentation* om te verwijzen naar locaties waar

digitale beveiligingstechnologieën kunnen worden geobserveerd, en bespreek ik twee methodologische uitgangspunten: (i) het volgen van digitale beveiligingstechnologieën van design tot gebruik en (ii) observatie van mens-computer interactie. Ten slotte bespreekt het hoofdstuk kort de validatie en beperkingen van het onderzoek.

In **hoofdstuk 4** wordt geanalyseerd hoe risicoprofielen van klanten tot stand komen, waarmee klanten worden bestempeld als "acceptabel" of "onacceptabel", gedurende wat banken "*the client lifecycle*" noemen. Deze cyclus omvat screening- en monitoringtechnieken die worden ingezet vanaf het moment van de *"onboarding"* van een klant tot het doorlopende klant- en transactiemonitoringproces, alsmede de mogelijke *"offboarding"*, oftewel het beëindigen van de relatie van de bank met een klant. Dit dynamische proces omvat risicobeoordelingen, het screenen van *watchlists*, het monitoren van transacties en handmatig onderzoek naar cliënten met een hoog risico. De bevindingen suggereren dat de procesmatige productie van een klantrisicoprofiel in toenemende mate afhankelijk is van openbare bronnen en van de gegevens die ten grondslag liggen aan digitale beveiligingstechnologieën. Het hoofdstuk toont bovendien aan dat *"know your data"* een steeds grotere rol speelt in de KYC-praktijken, met name wat betreft de kwaliteit van de data, de tijdelijkheid van data en data-gerelateerde aansprakelijkheid. Het hoofdstuk concludeert dat de oorsprong van veiligheidsbeslissingen ligt in vroege processen van data-organisatie en in de manier waarop digitale technologieën worden ontworpen en gebruikt.

In **hoofdstuk 5** wordt het begrip *de-scription* gebruikt om te onderzoeken hoe banken experimenteren met geautomatiseerde transactiemonitoringsystemen in een poging om terrorismefinanciering op te sporen. Allereerst analyseert het hoofdstuk de uitdaging om werkbare "input" te vinden voor transactiemonitoringsystemen, in de vorm van indicatoren van terrorismefinanciering. Banken experimenteren met het formuleren van deze indicatoren en met het afstemmen van de instellingen van hun transactiemonitoringsystemen. Het tweede deel bespreekt het design en gebruik van deze systemen aan de hand van drie *"scripts":* transactiemonitoring op basis van *rules*, modellen voor *supervised machine learning* en *unsupervised machine learning*. Het doel van al deze systemen is het opsporen van transacties met een mogelijk verband met terrorismefinanciering. Deze scripts lijken echter ook dilemma's op het gebied van privacy en ethiek op te werpen voor analisten bij banken. Bovendien suggereert de analyse dat geautomatiseerde systemen voor het monitoren van transacties in de praktijk ondoeltreffend kunnen zijn bij het detecteren van dreigingen van terrorismefinanciering.

Hoofdstuk 6 gaat over de uitwisseling van financiële *intelligence* met als doel terrorismefinanciering te bestrijden via publiek-private samenwerkingsverbanden. Het hoofdstuk gaat verder dan traditionele vormen van bestrijding van terrorismefinanciering en bespreekt experimenten met gerichte uitwisseling van intelligence in publiek-private samenwerkingsverbanden. Twee van dergelijke samenwerkingsverbanden

worden beschreven: één in het Verenigd Koninkrijk (JMLIT) en één in Nederland (de Terrorismefinanciering Taskforce). Publiek-private samenwerking maakt het voor de rechtshandhavingsinstanties mogelijk om tactische informatie te delen met banken die buiten het officiële strafrechtelijke onderzoek vallen, in een poging om terrorismefinanciering effectiever op te sporen. Uit het hoofdstuk blijkt dat *rule following* rond de bestrijding van terrorismefinanciering tot in de praktijk stand komt door een creatieve interpretatie en her-toepassing van bestaande regels. Dit proces lijkt zelfs de formulering van nieuwe regels te versnellen. Ik introduceer het begrip *"techno-legal gateway"* om aan te geven hoe de combinatie van technologische infrastructuur en juridische interpretatie nieuwe vormen van gerichte en genetwerkte uitwisseling van *intelligence* mogelijk heeft gemaakt.

Hoofdstuk 7 presenteert de conclusies van het onderzoek. Het geeft een overzicht van de belangrijkste bevindingen van het onderzoek, verkent de theoretische bijdragen van het proefschrift, identificeert maatschappelijke implicaties en doet suggesties voor toekomstig onderzoek. Het hoofdstuk gaat in op de substantiële inzet van personele en financiële middelen en de mate waarin dit bijdraagt aan de bestrijding van financiële criminaliteit, en concludeert dat het huidige systeem ineffectief en inefficiënt is. Er is een scheve verhouding ontstaan tussen de regelgeving die banken verplicht tot het opsporen en voorkomen van terrorismefinanciering, en de daadwerkelijke praktijk bij banken. Uit de analyse van de interacties tussen mens en technologie en van de data die ten grondslag liggen aan de veiligheidstechnologieën, blijkt dat het voor banken uiterst moeilijk is om in een patroon van financiële transacties de *intentie* tot financiering van terrorisme te ontdekken en dit vervolgens te *voorkomen*. Het hoofdstuk bespreekt de maatschappelijke implicaties, zoals de algemene gevolgen van grootschalig financiële *surveillance* voor de privacy van burgers (met risico op etnische of religieuze profilering), de onbedoelde gevolgen zoals *de-risking* en financiële uitsluiting, en de vervaging van de verantwoordingsplicht in steeds meer gedigitaliseerde veiligheidscontexten. Het is van belang om na te gaan met welk doel het instrumentarium voor de bestrijding van terrorismefinanciering wordt gecreëerd en of deze doelen worden bereikt. Uiteindelijk is de vraag welke rol private actoren zouden moeten spelen bij verreikende veiligheidsbeslissingen een politieke kwestie.

Acknowledgements

This thesis would not have existed without the support of friends, family and other individuals throughout my life who have helped me to arrive at a position from where I could start a PhD. For all their help during the PhD research and for making this journey such a pleasure, I am grateful to my supervisors, colleagues, and to all the research participants who have helped during my fieldwork.

First, I want to thank Marieke de Goede for being an incredible supervisor and for guiding me through academic life. Marieke, thank you for broadening my horizon and for all your valuable feedback, which was not only meaningful, constructive and well-timed, but also elegantly delivered. I am forever grateful for all the opportunities that you have given me, not least the chance to start the PhD. Polly Pallister-Wilkins, thank you for your supervision and for your all your feedback. Your encouragement has helped me to move beyond many stages of doubt during my research and to articulate my message to different audiences.

I would like to thank many people at the University of Amsterdam, beginning with the teachers I had during my time as a political science student. John Grin and Otto Holman, thank you for the inspiring lectures as well as for providing advice at crucial moments. Stephanie Simon, thank you for being my bachelor thesis supervisor and for suggesting that I could start the master track to continue in security studies. Geertje Haverkamp, thank you for being my first political science lecturer and then years later, for being there in the hallway when I was desperate to get into the masters programme. Many thanks to my colleagues at the Political Science department and others throughout the Amsterdam Institute of Social Science Research. My research has particularly benefited from generous feedback from colleagues of the Transnational Configurations, Conflict and Governance program group and the Global Digital Cultures research community. For some good conversations, I would specifically like to thank Huub Dijstelbloem, Evelyn Ersanilli, Meindert Fennema, Han van der Maas and Roderik Rekker.

It was great to be part of the research project FOLLOW. Rocco Bellanova, thank you for your feedback on many drafts and for sending me crucial pieces of old and new school literature. Pieter Lagerwaard and Tasniem Anwar, thank you for being fellow chain-members and for the many discussions, events, and lunches that we co-organised or participated in. It was also a pleasure to collaborate with friends of FOLLOW and those who have joined us along the way. Thank you Anthony Amicelle, Asma Balfaqih, Andreas Baur, Malcolm Campbell-Verduyn, Maja Dehouck, Marijn Hoijtink, Marie

Irmer, Beste İşleyen, Bruno Magalhães, Anneroos Planqué-van Hardeveld, Jasper van der Kist, Natalie Welfens, Mara Wesseling and Carola Westermeier.

I am grateful that much of my PhD had already taken place before the Corona pandemic began. Although ISA on Hawaii (!) was eventually cancelled in March 2020, I have been fortunate enough to be able to sharpen my thinking at many conferences and workshops in previous years. It was great to participate in the conferences organised by the European International Studies Association and the European Association for the Study of Science and Technology. The questions and feedback at the conferences as well as the quality time with those that have become more than just colleagues, were of great value.

Two workshops have been particularly important for me. FOLLOW's Secrecy & Methods workshop at the Teylers Museum in Haarlem was fun and a great team effort. It also laid the foundation for my thinking on secrecy, technologies, and methods. The conversations there eventually led to the volume *Secrecy and Methods in Security Research*. I am grateful to have been able to collaborate with all contributors to this book and for editing the volume with Marieke and Polly. I would also like to thank the participants of the Post-Critical IR workshop at PUC-RIO in Rio de Janeiro who have helped me to shape my academic positioning. My draft essay presented there, titled "Description is Critical Enough", did not make it into the final version of the thesis, but informs the foundation of the book and my general view of how I intend to practice science.

This thesis also benefited from a three-months research visit at the School of Political Studies at the University of Ottawa. Nisha Shah, thank you for being my third reader and for welcoming me into Canada and into the excellent and kind research community of Ottawa. And thank you William Walters for your feedback at various occasions and for organising the little workshop at Carleton University when I was in town.

My research has greatly benefitted from the generosity of my research participants who were willing to share their perspectives with me, ranging from cautious considerations to blunt opinions. I don't think it would have been possible to understand the practice of countering terrorist financing without the fieldwork that I have been able to carry out. Many thanks to everyone who participated via interviews, informal talks or by letting me observe their daily life within the bank. Following anonymisation guidelines, I will not thank anyone in name here, but if I could have, I would have!

Many thanks as well to everyone with whom I have enjoyed, coffees, lunch breaks, dinners and of course many 'borrels' (drinks). These moments were not only fun but were also often essential for creative thinking and for moving beyond writer's block. Thanks to my office mates in room 9.01 who have made daily life at the office such a pleasure: Astrid, Barbara, Bart, Chris, Daniel, Danny, David, Douwe, Edward, Jessica, Joep, Jos, Joshua, Kris, Kristin, Merel, Nilma, Pieter, Roberto, Selina and Tasniem. Thanks as well to the anonymous person who put the ping-pong table on the 10th floor.

Special thanks to Natalie, for all our conversations about academia, life, the messiness of everything and the good times; to Wouter, for our common teaching experiences and your sincerity; to Lilly, for the fun at the conferences and for the dialogues about humans, technology, and security; to Tasniem, for being that voice that I continue to take into account in my thinking; to Mara, for our joint fieldwork trips and your positive energy; to Joshua, for being my paranymph and for all our discussions about politics and practice and to Jasper, for being my intellectual companion since the very first workshop we visited and for the various laughing fits and shared self-mockery.

I am thankful for my family and friends and for their unconditional love and support. I would like to mention a few people in particular, without whom I probably would not have made it. Thank you Ko, for preventing me to drop out of university all those years ago; Eric, for providing the opportunity to continue; Miriam, for our common political science journey and container lifestyle; Erik, for the all the midnight phone calls; Natascha and Zinah, for keeping me sane through insane adventures; Paps en Mams, for your *vrijzinnigheid* and confidence in me; and Jáda, for being my sis and for being sharp or sweet based on whichever I need. And finally, thank you for everything, Pieter.

Banks have become private security actors. As "gatekeepers" of the financial system, they are legally obliged to conduct customer research and monitor bank accounts for unusual or suspicious transactions. If they identify transactions with potential links to money laundering or terrorist financing, they must report these to their national Financial Intelligence Unit. Because of the sheer volume of financial transactions that banks process daily, detection of financial crime relies on digital security technologies that help analysts categorise and identify risky customers and financial transactions. This thesis analyses how banks practice counter-terrorist financing and how they experiment with technologies to make authoritative security decisions.

Contributing to theories at the intersection of Science and Technology Studies and International Relations, the thesis develops a dynamic and processual understanding of risk detection and of processes of financial inclusion and exclusion. The research is based on fieldwork observations in the financial crime sector in the Netherlands and the United Kingdom. It includes three months' observation at a major Dutch bank, alongside interviews with public and private actors and document analysis. This dissertation analyses security at the human-technology interface, specifically during the production of customer risk profiles, in the design and use of transaction monitoring systems and in the emergence of public-private partnerships to counter terrorist financing. The research concludes that there is a misalignment between regulation and practice: the implementation of counter-terrorist financing rules does not lead to the effective prevention of terrorist financing in practice.