Multi-sited ethnography of digital security technologies

Bosma, E.

DOI
10.4324/9780429398186-19

Publication date
2020

Document Version
Final published version

Published in
Secrecy and Methods in Security Research

11

MULTI-SITED ETHNOGRAPHY OF DIGITAL SECURITY TECHNOLOGIES

Esmé Bosma[1]

- **Research objective**: This chapter will help researchers explore how they can study complex digital security technologies. The chapter delineates a multi-sited ethnographic approach around 'sites of experimentation'. It offers two methodological starting points: (i) following technology from design to use, and (ii) observing human-computer interaction.
- **Research puzzle**: The puzzle the chapter addresses in relation to secrecy and methods is: how can researchers make strategic use of their limited resources in order to understand, analyse and communicate to a wider audience the socio-political role of digital security technologies?

Introduction

"Who or what is responsible for the act of killing? . . . Which of them, . . . the gun or the citizen, is the *actor* in this situation?" (Latour 1999: 178–179). Bruno Latour, one of the main proponents of Actor-Network-Theory (ANT), famously mobilised the example of the gun to argue that technology is never just "a neutral carrier of human will" nor are we rendered powerless by its force. The mistake in both argumentations, argues Latour, is that they "start with essences, those of subjects or those of objects" (ibid.: 180). The outcomes of events are not entirely dependent on human or technological action. Rather, such outcomes lie at the intersection between human and non-human agency.

My research into counter-terrorism financing by banks is centred around the proposition to take seriously the role of 'non-humans' in security practice (see Box 11.1). I go beyond utopian and dystopian visions on technology to study: who and what is at work to counter terrorism financing? Security decisions are increasingly enacted via a combination of human and technological elements; they "transform, translate, distort and modify" the state of security affairs (Latour 2005: 39).

How does technology *mediate* decision-making by compliance professionals in banks when they anticipate, monitor, detect and report suspicions in the context of terrorism financing? In other words: how do banks know when money may be intended for facilitating a terrorist attack?

Banks make use of automated transaction monitoring systems to filter suspicious transactions. It is of increasing academic and societal relevance to provide more insights into the transaction monitoring and reporting practices of banks. This is because they are part of a *chain* of activities that may lead to security facts with powerful consequences (Amicelle and Iafolla 2017; De Goede 2018). Although they may eventually lead to the prevention and prosecution of terrorism financing, only a very small number of suspicious transaction reports actually lead to court convictions (Europol 2017). Critical questions have been raised about the effectiveness and effects of financial transaction monitoring such as financial exclusion and *de-risking* by banks of 'risky' regions, populations and non-profit organisations (De Goede and Wesseling 2018; HSC and ECNL 2018).

A growing body of literature at the intersection of International Relations (IR), (critical) security studies (CSS) and Science and Technology Studies (STS) has illuminated how security technologies, such as body scanners (Bellanova and Fuster 2013) and border detection devices (Bourne et al. 2015), transform how security expertise is being practiced and produced (Berling and Bueger 2015). As Bruno Latour points out:

> we have to accept that the continuity of any course of action will rarely consist of human-to-human connections (for which basic social skills would be enough anyway) or of object-object connections, but will probably zigzag from one to the other.
>
> *(Latour 2005: 75)*

This chapter draws on the ontological and epistemological insights from ANT, a strand of literature in STS, to outline a 'situated methodology' (Dijstelbloem and Pelizza, this volume). It will do so by suggesting some starting points for conducting detailed empirical investigation into digital devices across multiple "sites" (Latour 2005: 219).

I delineate a multi-sited ethnographic inquiry of digital security technologies centred around *sites of experimentation*. Within this chapter, I refer to these sites as settings in which the (potential) role, as well as the ethical, technical and practical dilemmas of the design, implementation and use of digital security technologies are openly discussed. Digital security technologies pose particular secrecy challenges for researchers. They are often privately owned, localised in numerous sites and are used in combination with sensitive data. Moreover, it requires specialised knowledge to elucidate technologically-mediated security practices (Van Veeren 2018; see introduction to this volume). Although an abundance of studies have demonstrated the crucial role and political effects of digital and material security devices (see, for example, Amicelle et al. 2015 or Suchman et al. 2017), the methodological choices and challenges of conducting a detailed empirical analysis of these complex

technologies often remain implicit. The main question that this chapter aims to answer is: how can we account for the productive role of digital security technologies in effecting judgments and decisions in the security realm?

For researchers with a non-technical background, it is especially difficult to decide how much understanding of the actual workings of these complex technologies is needed in order to be able to attain a realistic impression of the dynamics of human and non-human agency that make up security practices. The chapter will help researchers to make strategic choices to align background knowledge and expertise with research objectives. It offers theoretical and practical suggestions to understand, analyse and communicate to a wider audience the socio-political role of digital security technologies.

The chapter commences by delineating a methodological approach for studying digital security technologies. The chapter consists of three parts. The first part discusses the secrecy challenges of digital security technologies and outlines how a multi-sited ethnographic approach centred around sites of experimentation can help to study them, but also what the challenges might be. In the second and third parts, I draw upon my personal research experiences to develop and illustrate two methodological avenues – or rather starting points – for conducting ethnographies of digital technologies: (i) following technology from design to use and (ii) observing human-computer interaction.

BOX 11.1 COUNTER-TERRORISM FINANCING BY BANKS

Starting in 2017, my research has primarily focused on counter-terrorism financing efforts by major banks in Europe. By conducting ethnographic research in and around banks, the study addresses how compliance professionals navigate the complex and occasionally competing responsibilities of their security, commercial and societal roles. My research not only analyses how human backgrounds, expertise, habits, routines and inclinations come to matter in a daily context, but also incorporates human interaction with security technologies and the subsequent ethical, technical and practical dilemmas practitioners face.

Inspired by insights from STS and CSS, the study foregrounds the role – and reliance on – digital technologies in the production of security expertise by compliance officers and intelligence analysts in financial institutions. Following what Latour has called the "making of" (Latour 2005), I investigate suspicious transaction reports through combined action by humans and non-humans. Deploying the notion of *de-scription* (Akrich 1992), furthermore, my aim is to follow – non-sequentially – the evolution of transaction monitoring software and/or machine learning algorithms, from its very design to use in practice.

My research has (so far) been conducted in the Netherlands and United Kingdom. It includes 60 interviews – ranging from long formal conversations to semi-structured interviews – with amongst others compliance professionals, consultants, law enforcement representatives and regulators. I have also interviewed IT experts, data scientists, software engineers, product developers and analysts that were somehow involved in the workings of the transaction monitoring system – either by inscribing its input or processing its output. I have undertaken fieldwork at a wide range of information and stakeholder sessions about financial crime including three national workshops and one international anti-money-laundering conference.

A considerable part of my ethnographic data derives from one Dutch bank, where I have conducted a three-month research internship between March and June 2018. Following extensive negotiations concerning, for example, the objectives of my research and anonymity and confidentiality (see De Goede, this volume), I received access to experience first-hand the professional lives of compliance professionals. For three months I was an 'intern' observer, slowly mapping and developing an in-depth understanding of the dilemmas practitioners face concerning the countering of terrorism financing. I was based at the compliance department, from where I 'snowballed' through various other departments of the bank, conducting observations and interviews as I went.

Studying digital security technologies

In an increasingly data-driven world, the innovations of Artificial Intelligence (AI) and computer science have led to new ways of securing and governing populations. Security and intelligence professionals in law enforcement, border control and in private contexts such as banks make discretionary decisions in dialogue with security devices (Amicelle et al. 2015). This part discusses the methodological challenges and opportunities of studying digital security technologies. In the first section I briefly present the case of transaction monitoring systems. Then I discuss which secrecy challenges digital security technologies pose. In the last two sections I delineate a multi-sited ethnographic approach focusing on sites of experimentation.

The case of transaction monitoring by banks

Financial institutions such as banks have the legal obligation to act on "the prevention of the use of the financial system for the purposes of money laundering or terrorist financing" (Directive (EU) 2018/843). They need to comply with international 'customer due diligence' (CDD) standards to know, identify and verify customers and beneficial owners of companies and conduct a risk assessment before

accepting customers. On a regular basis they have to monitor and review whether clients behave according to their 'risk profile' by checking their accounts and monitor transactions for unusual and suspicious financial behaviour. Unusual and/or suspicious transactions have to be reported to Financial Intelligence Units (FIUs).

To identify terrorism financing, transaction monitoring systems are used, that need input in the form of 'scenarios' (DNB 2017b). For a 'terrorism financing scenario', one has to formulate certain indicators. Based on scenarios and threshold values, the transaction monitoring system filters out unusual (or suspicious) transactions and generates alerts. Indicators, for example, could be formulated according to the type of customer, customer segment, the earlier formulated 'risk profile', geographical location and cash or wire transactions. An example of such a 'business rule' in the retail segment of banks is: "customers within a specific age group, e.g. 18–25 years, crossing certain limits with respect to the size and frequency of non-cash transactions" (DNB 2017b: 23). Major banks employ hundreds of analysts who manually process the automatically generated alerts. They conduct research into the customer's or company's general profile, bank accounts and transaction behaviour and possibly report it as unusual.

Despite the implementation of automated transaction monitoring systems, the Dutch Central Bank (DNB) concludes that "financial institutions in all sectors manage the risk to become involved in terrorist financing insufficiently", stating that "the transaction monitoring systems are often insufficiently tailored to detect terrorist financing and deficiencies are regularly found in client research" (DNB 2017a). For banks, failing to report or reporting too quickly can have financial but also reputational consequences. Many major banks have paid millions in fines or settlements after allegations of insufficient anti-money laundering controls (for example De Clerck and Bové 2017; FCA 2017; Klumpenaar 2015; OM 2018).

The identification of unusual or suspicious transactions in relation to terrorism financing creates difficulties as they are often small, mundane transactions that do not stand out (De Goede 2017; NVB 2017). There is a lack of concrete indicators for terrorism financing that can be translated into scenarios and business rules. A problem often mentioned in the compliance sector is that the monitoring system generates too many transactions that are falsely flagged as unusual or suspicious ("false positives"). This creates a compliance overload:

> The whole movement in the market simply indicates, that in the traditional model, of "we set the scenarios, and we process the alerts", everyone gets swamped. It does not work. So everyone is looking at alternative solutions such as algorithms and machine learning algorithms. That is really unavoidable.
>
> *(Interview bank employee, 2018)*

AI and machine learning technologies are increasingly seen as an answer to the growing pressure on banks and relating compliance personnel costs. They are advertised in practitioners' magazines with covers like "Look past 'wow' and see hope for compliance overload" and "Up to speed on Artificial Intelligence?" (Banking

Exchange 2017). Companies offer machine learning tools for financial crime professionals promising "compliance by design", "greater operational effectiveness" and "advanced analytics". Researchers who aim to analyse the role of these complex technologies may be confronted with practical and technical challenges.

Secrecy and digital security technologies

Numerous scholars have deployed STS insights into their respective fields to study the complex socio-material nature of digital technologies. Intersecting STS with law and philosophy (Hildebrandt and Rouvroy 2011), communication and media studies (Gillespie 2014), surveillance studies (Kroener and Neyland 2012), and Human Computer-Interaction studies (Suchman 2007), they have successfully shown how the study of algorithms, autonomic computing, software and technological change can provide an entry-point to study power, agency, accountability and human autonomy. In security studies too, it has been shown that the deployment of algorithmic techniques for security entails important political and ethical stakes that should be described and analysed (Amoore and Raley 2017; Aradau and Blanke 2015; Grommé 2016; Kaufmann et al. 2019). But digital security technologies may be hard to comprehend. Whether there is an interest to study technology from the start, or whether awareness of mediating technologies arises later on in the research process, one can get easily overwhelmed by the technological jargon, buzzwords and rapid innovation in the tech-world (see Box 11.2). In particular for researchers with limited technical expertise, this is a time-consuming challenge.

BOX 11.2 AN ETHNOGRAPHY OF WHICH TECHNOLOGY?

Ethnographic research can seem deceptively simple. "It may appear to require only that one 'act naturally', putting aside any methodological rules and constraints" (Hammersley and Atkinson 2007: 21). For researchers who are not trained in anthropology and perhaps have received limited ethnographic training, it is important to reflect upon some of the common problems within ethnographic research designs, such as defining a viable research problem (ibid.: 21–40).

According to Bruno Latour: "*any thing* that does modify a state of affairs by making a difference is an actor" (Latour 2005: 71, emphasis in original). Although I was interested in the automated software that makes a selection of potential suspicious transactions, I encountered many other technologies that were potentially mediating security practices by banks.

That is when I started to perceive many more actors. Questions arose such as: what is an algorithm? What is a transaction monitoring system? What is

machine learning and Artificial Intelligence and what are the differences? How can they be used to spot terrorist activity within financial data? Can they? Who is making this software? What does a data scientist do? What is blockchain? What are cryptocurrencies?

Posing and answering such questions may be helpful for understanding the technology under investigation and may lead to surprising research opportunities and findings. When explored exhaustively, however, one might face the danger of drowning in technical details, losing focus and being distracted from the initial research question.

Banks may develop their own in-house transaction monitoring systems, yet often buy (expensive) software packages from external vendors such as LexisNexis, Oracle, Palantir, SAS or Worldcheck. Private actors will often guard the precise workings of the algorithms as a secret, as they are a fundamental part of the company's business model which enables them to develop a competitive advantage (Gillespie 2014). Even if one would have access to the algorithmic codes, it requires specialised knowledge to be able to understand them. Furthermore, it is nearly impossible to know how they would work in practice as their productivity only becomes apparent *after* implementation and in combination with data.

Other chapters in this volume discuss challenges around gaining access, confidentiality and research ethics in different settings (see De Goede, this volume, about the process of gaining access to the bank). It should be noted here, however, that working in the context of counter-terrorism is particularly challenging; a blue-print of counter-terrorism financing policies and practices cannot end up in the public domain. Hypothetically though, one can wonder to which extent the often partial and situated knowledge could pose a security risk. Although scattered, much information already exists in the public domain in policy reports, conference presentations, published minutes, user guides of technologies and so on. During my fieldwork I was open to my respondents about my research interests as well as in which I was *not* interested. Every time I explicated that I was not interested in personal and sensitive customer data, but in dilemmas and daily practices. Still, encountered sensitive data as well as working practices too precise to publish can function in different ways, for instance as background information to make sense of processes.

One of the challenges of studying digital technologies is that they consist of more than computer codes; they are made of "stuff" too (Dourish 2017). For instance, the material infrastructures supporting the virtual or the data (like computers, screens, cables, servers and electricity networks) can either enable or constrain the workings of a software programme (Amoore 2016). Understanding, perhaps even finding the technologies, is further complicated by the emergence of sophisticated security devices such as surveillance cameras, biometric identification and verification

systems and transaction monitoring systems that operate through AI and machine learning algorithms such as anomaly detection or 'neural networks' (Vayre 2018; see also Straube, this volume).

In his ethnographic study of risk-calculation and data-driven governance by the British Fire and Rescue Service (FRS), Nathaniel O'Grady (2015) demonstrates how data and digital technologies can simultaneously be free-floating, as well as dispersed and localised into various contexts. The analysis software MOSAIC, previously used by credit checking company Experian to profile populations in terms of consumer behaviour, was acquired and *redeployed* by the FRS to establish risk profiles of people most vulnerable to fire. Through conducting detailed empirical investigation into the "processes of appropriation, localisation and redeployment", O'Grady shows how digital risk calculation technologies "must undergo transformation to adapt to new organisation sites and spaces before enacting new modes of governance" (2015: 82). A digital security technology can be appropriated and transformed into numerous sites such as the military, intelligence agencies, police departments and private security actors across the globe. Although the dispersed nature of data and their associated software appears to add to their ungraspable nature, I argue that the moments in which the technology travels to new contexts offer opportunities for ethnographic research accounts of digital devices. As noted by O'Grady: "[c]ritical accounts of data-driven governance (. . .) must examine the mundane organisational routines, practices and processes that facilitate technological redeployment" (ibid.).

Multi-sited ethnography

How can complex digital security technologies be incorporated into an ethnography? And in which field should the fieldwork take place? There is a growing literature on digital ethnographic methods. Some studies focus on data collection in the "virtual field" (Hammersley and Atkinson 2007: 137; Lazar et al. 2017: 252), others make the digital device the prime object of analysis (Amoore and Raley 2017; Aradau and Blanke 2018; Ziewitz 2016).

In a "multi-actor and multi-level technopolitical context" new political entities arise that transcend the 'state' (Dijstelbloem and Pelizza, this volume). Terrorism financing is a security problem that transcends national borders as well as boundaries between the public and private realm. Most banks are transnational corporations operating within multiple jurisdictions. Financial anthropologists have studied global financial processes of localisation and appropriation: "financial practices do not diffuse globally in a uniform manner, but are instead utilised locally in a specific way" (Lagerwaard 2015: 575). Transaction monitoring systems are being produced by major technology firms that compete in the global market and are localised into many contexts. This dynamic context asks for a flexible approach that combines multiple ethnographic methods of data collection at multiple sites (Baird 2017; Cohn 2006; Marcus 1995; Schwell, this volume).

In order to develop an initial understanding of the security responsibilities of financial institutions before my internship in the bank, I used techniques of

unstructured observation. Researchers using unstructured observation "are seeking to be taught by the world and want to get as close to the reality of the events as possible without being so constrained by preconceived notions of how things work that they overlook some important aspects" (Manheim et al. 2012: 333). Unstructured observation may seem trivial, but it allowed me to gain a sense of the field, as well as to have many conversations with bankers, compliance professionals and tech-companies – thereby making it a part of my ethnography as well as a snowball-sampling method. Although I was attentive to the role of security technologies from the beginning, my research does not focus exclusively on technologies (see Box 11.1).

In the beginning of my ethnography in the bank I spent a considerable amount of time just 'being' in the bank to learn about the myriad of security issues the bank deals with next to terrorism financing: various types of fraud, money laundering, corruption, violence to ATM machines, information security, the safety of employees at the office as well as abroad, data leaks and so on. I engaged with compliance professionals around me, read reports and guidance documents and followed online training. Taking the opportunity to experience the daily life at a compliance department, I spent most of my time sharing coffees with employees, joining and observing meetings whilst arranging a series of interviews.

I read secondary academic literature, policy reports, media-articles and practitioners' magazines about compliance and banking and I also signed up for forums, blogs, newsletters and event alerts of relevant public actors, companies and anti-financial economic crime organisations. This created a constant stream of information about issues and events at the intersection of security, technology and finance. Sometimes I went to rather generic technical workshops, for instance on blockchain technology. Other times, I went to more specialised events around my topic such as one on detecting financial crime with machine learning for financial institutions. At such meetings I often asked technical experts to explain in clear language the workings of digital technologies. Although this led to a general understanding of the technologies at play, I felt that in order to show how the transaction monitoring system 'acts', a more detailed understanding of the inner workings of the technology was necessary.

In a first attempt to studying machine learning algorithms that are being used to identify financial economic crime, I tried to "reflexively produce code", an approach of researching algorithms whereby the "researcher reflects on and critically interrogates their own experiences of translating and formulating an algorithm" (Kitchin 2017: 23). In short, I learned quickly that this was not feasible. Because of the variety of algorithms, programming languages and strands of computer and data science, it was unclear which 'code' to study and where. This problem was even further complicated by my limited experience in programming or coding and pre-existing technological knowledge. Till Straube (this volume) convincingly problematises 'opening the black box of algorithms'. In the next section I show that there are indeed "other ways to situate the device, other paths of inquiry to follow" than to study the inner workings of the algorithm (Straube, this volume).

Sites of experimentation

Where can digital technologies be observed and analysed? Based on theoretical and methodological perspectives originating in ANT research, I propose to conduct ethnographic research at sites of experimentation, termed as settings in which the (potential) role, as well as the ethical, technical and practical dilemmas of the design, implementation and use of digital security technologies are openly discussed. Although they shape our lives in numerous ways, most technologies run 'silently' (Latour 1992) in the background. We do not treat them as mediators that *do something* (Latour 2005: 128), but as intermediaries or *black boxes*; "defining its inputs is enough to define its outputs" (Latour 2005: 39).

ANT accounts therefore study occasions during which facts or artefacts are not (yet) stable and taken-for-granted (Latour 2005: 79). It is during the moments that the technology is being developed or breaks down – or indeed as O'Grady demonstrated, when it is being appropriated, redeployed or localised into new contexts – that technologies are present and visibly active. Traditionally, much STS and ANT research has therefore revolved around experiments and in the laboratory (Latour 1999; Sismondo 2010). Daniel Neyland illustrates how projects of experimentation with technology can provide fruitful terrain for ethnographic research into digital devices: "algorithms and their system are continually inspected and tested, changed and further developed" (2018: 22). He argues that to study the 'everyday life of algorithms', one should "pay attention to the everyday work required for algorithmic conditions and consequences to be achieved" (Neyland 2018: 32).

Digital security technologies are actually continuous objects of experimentation: there are many people at work in the design, implementation, 'tuning' and use of the technology (Weber 2016). It is in these moments of experimentation that the technology and the way in which it transforms of modifies a state of affairs becomes less taken-for-granted and opaque; the technical characteristics, practical dilemmas and often ethical issues are openly discussed. As I show in this chapter, the transaction monitoring system too, is a continuous object of experimentation. There are many people at work that aim to optimise the filtering of suspicious transactions out of millions or regular commercial transactions. According to Annemarie Mol, ANT researchers do generally emphasise the work involved in ordering. Mol argues that "when norms have been set, 'normalisation' does not automatically follow" (Mol 2010: 263). Building on insights from Michel Foucault, forms of ordering are not the 'product of centralised deliberation' or a 'strategic subject', but "spread themselves through and pattern the fabric of the social to operate as a microphysics of power" (Law and Ruppert 2013: 231).

In the following two sections of this chapter I describe two methodological starting points for researchers who are interested in conducting ethnographies of digital technologies. In the next section I suggest that in order to identify sites of experimentation, a methodological starting point could be to follow technology from design to use. This will enable to see who and what is at work in ordering society. In the final section, I provide practical tips for studying the use of digital technology at a specific

site; for observing human-computer interaction. Finding instances and 'sites' of experimentation around your digital technology of interest is a way to identify moments in which the workings and dilemmas of the digital technology may become apparent.

Digital security technologies from design to use

Studying technology from design to use allows to study the different human and non-human *actors* involved in the enactment of security decisions and to identify sites of experimentation; the moments in which the technology becomes visible. In *The De-scription of Technical Objects*, Madeleine Akrich famously shows how technical objects form part of a chain: "although they point to an end, a use for which they have been conceived, they also form part of a long chain of people, products, tools, machines, money, and so forth" (1992: 205). ANT has shown how beneficial it is to conduct ethnographies of technologies during the "making of" phase (Latour 2005: 89), when the facts and artefacts have not yet been stabilised. In the previous section, I argued that sites where technologies are being 'tuned' and used can be equally interesting and useful. However, "construction sites" (Latour 2005: 88) or sites of experimentation are not always easy to locate. How does one go about research when they are not clearly demarcated in the form of an experimental project around the development of a new technology? In this section, I suggest a non-sequential approach through which to follow the technology from design to use, moving through different phases of experimentation.

In order to know about the 'making-of' transaction monitoring software systems, one would have to "loop back" (Bourne et al. 2015) to the designers (i.e. software developers) of large companies. As banks employ often thousands of people, it is difficult to know which forms of transaction monitoring they use, who designed it, and who uses it. Like many other (digital) security technologies, financial transaction monitoring systems are often being sold in the form of a finished product whereby it is difficult to recognise the original designers or engineers. This poses challenges around access and secrecy and to the feasibility and scope of the research project. Likewise, it may be complicated to find out if and where banks are developing in-house transaction monitoring systems or machine learning tools.

As previously mentioned, the localisation of digital security technologies into different organisational contexts raises questions about where an ethnography of the digital might take place. One of my solutions to identify sites of experimentation was to visit a specialised conference on anti-money laundering and counter-terrorism financing. Attending the panels and workshops provided more insights into the socio-technical characteristics, possibilities, and challenges of transaction monitoring systems. In a specific area of the conference, numerous software companies and vendors advertised their products to the bankers and compliance officers attending the conferences (see also Baird 2017; Hoijtink, this volume). I collected sales folders, spoke with salespeople about the possibilities of their products, saw demos, shared and 'tested' my research interests, assumptions and understanding of technicalities with a technical crowd.

Security conferences and fairs are useful sites where one can learn about the different stakeholders who are involved in designing, developing, selling, acquiring, implementing, maintaining or 'tuning' of transaction monitoring systems: lawmakers, software vendors, directors and managers of financial institutions, consultants, compliance officers, IT experts, data scientists and so on. Rather than studying one project, I learned about the plethora of instances – of tuning and experimentation – in which sovereign decisions are inscribed into transaction monitoring systems. Multiple times I encountered 'product owners' of transaction monitoring systems. 'Product owner' is a term that is often being used in (tech) companies, start-ups and IT development frameworks. Although they may have different tasks, product owners are often in charge of a certain (IT) 'product'; they keep oversight, supervise a team responsible for development and implementation and communicate with customers and/or stakeholders. Product owners of transaction monitoring systems in financial institutions are responsible for the operational workings of the system; they implement and 'tune' scenarios and maintain and evaluate the systems. Interviewing product owners can provide a good insight into the technical workings of the system as well as the socio-political dilemmas of detecting financial crime.

Instead of sticking narrowly to a sequential approach from design to use, I propose to use it as a thought construct to help identify sites of experimentation (see Box 11.3). The methodological starting point is to put the socio-technical characteristics of the digital security technology center stage. From there we can "loop back" (Bourne et al. 2015) into the processes of technological development and 'loop forward' into its appropriation by end-users in practice. Moreover, "[r]ather than holding stable and separate the identities of 'designer' and 'user'", as Lucy Suchman has argued, they should work as "categories describing persons differently located, at different moments, and/or with different histories and future investments in projects of technology development" (2012: 57). This will help researchers to map the socio-technical assemblage (Kitchin 2017) of digital security technologies.

BOX 11.3 QUESTIONS TO CONSIDER WHEN FOLLOWING TECHNOLOGY FROM DESIGN TO USE

- What is the socio-political context of the digital device? For which problem should it offer a solution?
- Who are or have been involved in designing, developing, selling, acquiring, implementing of the technology and who uses it?
- In which organisational context is the technology being appropriated, redeployed and localised?

- What are the socio-technical characteristics of the digital device? (What does it do and when does interaction with humans take place?)
- Which ethical, technical and practical dilemmas of the security technology do designers, users and other stakeholders mention?

Observing human–computer interaction

One instance in which the workings of digital security technologies may become visible is in its use by security professionals. To study technology in use (especially new users) has been a long tradition in STS and ANT to unpack routine and taken-for-granted technologies (Verbeek and Slob 2006). Analysts can temporarily create the same type of novelty through "irruption into the normal course of action of strange, exotic, archaic, or mysterious implements" (Latour 2005: 80). One way for irruption into the normal course of security decision-making is to make this interaction between the human and computer – the use of a technology – a primary ethnographic focus; to regard the security professional behind a computer as a site of experimentation. Transaction monitoring systems can be considered as continuous objects of experimentation because the system is constantly adapted to evolving security threats, technological innovation as well as feedback from analysts about the effectiveness of the output. Periodic feedback offers incentives to 'tune' the system in other ways.

The human–computer interaction (HCI) literature, of which a comprehensive overview cannot be given here, presents empirically rich and interesting accounts of the human-machine interface. Although a part of HCI specifically explores design and use of technologies and interfaces for purposes of product development – not necessarily a research goal for security researchers – the wide variety of methods such as interviews, research diaries, focus groups, case studies, ethnographies and 'user-research' deployed in HCI can provide inspiration to study human-computer interaction in security contexts (see for an overview Lazar et al. 2017). Consider for instance Lucy Suchman's (2007) – originally published in 1987 – seminal ethnographic study of user interaction with a newly developed photocopy machine. Also, her later work on tracking and targeting technologies should be noted here (Suchman et al. 2017). This chapter focuses on the observation of human-computer interaction behind a desk. Sometimes, the observation of human–computer interaction can happen unexpectedly, when respondents spontaneously show things on the screen. At other times, the interaction in itself can become the object of longer ethnographic research (see the chapters on 'case studies' and 'ethnography' in Lazar et al. 2017). In my case, it was a small part of a broader ethnographic study of the security responsibilities of banks.

Observing 'the processing of alerts'

In order to understand the possibilities and difficulties in detecting terrorism financing by banks, the transaction monitoring system had become an object of

interest for my research. The accuracy of the alerts - the output of the system - provides input for the those with the task to 'tune' the system. The processing of alerts can therefore be considered as continuous experimentation. As one bank employee put it during an interview:

> The moment you set your thresholds too weak, you miss out on a lot and are not doing well. Of course we have a moderate risk appetite, so we prefer to set our thresholds too tight, so we get a lot of alerts, but if you have so many alerts that at a given moment, to say it very directly, you drown in the alerts, [. . .] that is also not the aim. That is really a dilemma, how do I set my thresholds, how do I optimally tune.
>
> *(Interview bank employee, 2018)*

Through observing the output of transaction monitoring systems and the processing thereof, I aimed to learn more about the supposed difficulties in detecting financial economic crime and terrorism financing in specific, as well as about the daily dilemmas of compliance professionals. Inspired by often empirically rich ANT studies of 'chains of translations' (Latour 1999), my aim was in addition to observe and document a typical step-by-step processing of an alert; the analyst 'in dialogue with' the transaction monitoring system. One day, a manager arranged for me to sit next to an analyst for the day.

With quick mouse-clicks switching into different interfaces, it was hard to follow the different steps in the process and the discretionary choices that were made. Next to the transaction monitoring system, analysts use a variety of software programmes and tools to assess if the alert on the unusual transaction is an example of unusual or suspicious behaviour that should be reported. It was impossible just to be an observer. I felt like a nuisance since I interrupted the analyst with numerous questions about every little step.

A lot of work in banks takes place behind a computer, tablet or cell phone. What is being viewed, decided or done is not easily observable. Whereas the use of some mundane technical objects (like the photocopy machine) is clearly visible, this is not the case when financial analysts and compliance officers in banks interact with their screens. After all, how would an ethnographer be able to study me when I do research? Although a large part of it takes place behind a computer, one would get a very partial idea of my daily practices by just sitting next to me for an afternoon, or even a week.

Looking back at my extensive field notes of that day, it is clear that the observation has been crucial to my understanding and analysis of daily security practices in banks. For instance, through observing interaction with the screen I learned about the various software programmes that are being used, the types of data that analysts work with and typical actions to process alerts. In addition to the interaction with the screen, I documented the daily life and routines of analysts, the communication lines and the differences between departments within the bank (i.e. compliance, the

business lines etc.), the frequency and nature of unusual transactions in relation to various financial economic crime profiles, the challenges of analysts and their recommendations for improvement. In combination with other interviews, it allowed me to gain a broad sense of the technological possibilities and challenges in detecting terrorism financing.

However, given the fact that I had only one day for observation, it had been unrealistic to expect to document a precise step-by-step processing of an alert in addition to the wider social context of the analysts. First, human–computer interaction is a quick and fleeting moment that is difficult to capture. It was impossible to document the sequence of interaction as there were too many interactions with too many software programmes. To document one's own first encounter with a security technology at the same time is challenging at the least. Second, with unrealistic research objectives and by sticking frenetically to Latour's lesson on taking field notes and research diaries and his warning that "everything is data" (2005: 133), I had put both myself as well as the analyst under pressure to capture every little detail.

It is important to reflect on such research 'failures' as it can be revealing in itself to document the complexity of security technologies and the ways in which secrecy has a productive effect on researcher and researched (see introduction to this volume). Also, it contextualises the data that was obtained as well as the credibility of the research account. Whereas in human-centred ethnographies one can go back to the respondents to verify constructed realities (Guba and Lincoln 1989), this is not the case when interaction is the research objective. In my case, it was only the combination with ethnography of the human part of the interaction and the wider social context that provided insights into the enabling or constraining potential of transaction monitoring systems. With sufficient preparation, realistic expectations and a research design that balances structured and unstructured elements however, there is much to be gained from observing human-computer interaction (see Box 11.4).

BOX 11.4 QUESTIONS TO CONSIDER WHEN THINKING ABOUT OBSERVING HUMAN-COMPUTER INTERACTION

- What are you interested in *precisely*? In the perspective of the human, their interaction with the computer, or the socio-technical characteristics of a specific programme?
- How will you communicate your research interests to your respondent?
- Who will you observe and "how is the research process shaped by the relationship between you as a researcher and your participants?" (Nyman, this volume)

- In which setting will you observe human–computer interaction? (the respondent's role in the organisation and physical location might influence your observations: sounds, privacy, visibility, other colleagues, etc.)
- Which role (participant and/or observer) will you take?
- How much time will you have for observation and what is a realistic research goal for this duration?
- How are you going to take notes and what kind of notes will help you answer your research questions at a later stage?
- Will you encounter sensitive data? Is there privacy-sensitive or confidential information that you should leave out of the analysis/anonymise?
- Would it be useful and possible to have a preparatory meeting with the person behind the computer?
- Will you be able to do "member checks" to verify your assumptions and descriptions in the form of a debrief or interview afterwards and if so, what will you check? (Guba and Lincoln 1989: 239).

Conclusion

This chapter has shown why it is fruitful to conduct an ethnographic investigation of digital security technologies. Studying digital security technologies poses particular challenges of secrecy, because they are often privately owned, localised and embedded in many different contexts. Multi-sited ethnography can help to account for the productive role of complex and digital security technologies. Drawing on my own research experiences of studying transaction monitoring systems used by banks to counter-terrorism financing, I have illustrated how sites of experimentation can be fertile grounds for ethnographies of technologies. An iterative and (un)structured research process becomes even more rewarding when combined with continuous reflection on research objectives and scope. The chapter offers two concrete ways in which one might approach and study obfuscated digital technologies, being (i) to follow digital security technologies from design to use and (ii) to observe human–computer interaction. These methodological starting points will help researchers to conduct detailed empirical inquiry into the role of non-human actors in security practices. However, when putting technology centre stage, we should keep in mind not to be glued to it, but to trace its connection through and into the world.

Suggestions for further reading

- Madeleine Akrich (1992) "The de-scription of technical objects", pp. 205–224 in Wiebe. E. Bijker and John Law (eds) *Shaping Technology/Building Society: Studies in Sociotechnical Change*. Cambridge, MA: MIT Press.

- Mike Bourne, Heather Johnson, and Debbie Lisle (2015) "Laboratizing the border: The production, translation and anticipation of security technologies", *Security Dialogue*, 46(4): 307–325.
- Bruno Latour (2005) *Reassembling the Social. An Introduction to Actor-Network-Theory.* Oxford: Oxford University Press.
- Edwin Sayes (2014) "Actor–network theory and methodology: Just what does it mean to say that nonhumans have agency?", *Social Studies of Science*, 44(1): 134–149.
- Malte Ziewitz (2016) "Governing Algorithms: Myth, Mess, and Methods", *Science, Technology, & Human Values*, 41(1), 3–16.

Note

1 Acknowledgements: thanks to Tasniem Anwar, Rocco Bellanova, Marieke de Goede, Hendrik Ike, Pieter Lagerwaard and Polly Pallister-Wilkins for the reading tips, helpful comments and support during the research and writing process. My sincere gratitude goes out to the many employees at The Bank for the kindness, trust and support during my fieldwork period and to all the other respondents who shared their valuable perspectives.

References

Akrich, Madeleine (1992) "The de-scription of technical objects", pp. 205–224 in Wiebe. E. Bijker and John Law (eds) *Shaping Technology/Building Society: Studies in Sociotechnical Change*. Cambridge, MA: MIT Press.

Amicelle, Anthony, Claudia Aradau, and Julien Jeandesboz (2015) "Questioning security devices: Performativity, resistance, politics", *Security Dialogue*, 46(4): 293–306.

Amicelle, Anthony and Vanessa Iafolla (2017) "Suspicion-in-the-making: Surveillance and Denunciation in financial policing", *The British Journal of Criminology*, 58(4): 845–863.

Amoore, Louise (2016) "Cloud geographies: Computing, data, sovereignty", *Progress in Human Geography*, 42(1): 4–24.

Amoore, Louise and Rita Raley (2017) "Securing with algorithms: Knowledge, decision, sovereignty", *Security Dialogue*, 48(1): 3–10.

Aradau, Claudia, and Tobias Blanke (2018) "Governing others: Anomaly and the algorithmic subject of security", *European Journal of International Security*, 3(1): 1–21.

Baird, Theodore (2017) "Knowledge of practice: A multi-sited event ethnography of border security fairs in Europe and North America", *Security Dialogue*, 48(3): 187–205.

Banking Exchange (2017), June/July edition, available on: https://issuu.com/banking-exchange/docs/banking_exchange_june_?e=16540037/49780807 (accessed 8 February 2019).

Bellanova, Rocco and Gloria G. Fuster (2013) "Politics of disappearance: Scanners and (unobserved) bodies as mediators of security practices", *International Political Sociology*, 7(2): 188–209.

Berling, Trine V. and Christian Bueger (eds) (2015) *Security Expertise: Practice, Power, Responsibility*. New York: Routledge.

Bourne, Mike, Heather Johnson, and Debbie Lisle (2015) "Laboratizing the border: The production, translation and anticipation of security technologies", *Security Dialogue*, 46(4): 307–325.

Cohn, Carol (2006) "Motives and methods: Using multi-sited ethnography to study US national security discourses", pp. 91–107 in Brooke A. Ackerly, Maria Stern and Jacqui True (eds) *Feminist Methodologies for International Relations*. Cambridge, UK: Cambridge University Press.

De Clerck, Gwend and Lars Bové (2017) "Arrest zet witwasmeldingen banken op de helling", *De Tijd*, 20 May 2017, available at: http://www.tijd.be/ondernemen/banken/Arrest-zet-witwasmeldingen-banken-op-de-helling/9896319 (accessed 8 February 2019).

De Goede, Marieke. (2017) "Banks in the frontline: Assembling space/time in financial warfare", pp. 119–144 in Brett Christophers, Andrew Leyshon and Geoff Mann (eds) *Money and Finance After the Crisis: Critical Thinking for Uncertain Times*, Hoboken, NJ: John Wiley & Sons.

De Goede, Marieke (2018) "The chain of security", *Review of International Studies*, 44(1): 24–42.

Dourish, Paul (2017) *The stuff of bits: An essay on the materialities of information*. Cambridge, MA: MIT Press.

DNB (De Nederlandsche Bank) (2017a). Position paper for the roundtable discussion on countering terrorism financing, Committee on Finance, Dutch House of Representatives, The Hague, 7 February 2017, available at: https://www.dnb.nl/binaries/PPterrorismefinanciering_tcm46-352386.pdf?2018090513 (accessed 7 February 2019)

DNB (2017b) "Post-event transaction monitoring process for banks", Guidance, pp. 1–48, Amsterdam, 30 August 2017, available at: http://www.toezicht.dnb.nl/en/binaries/51-236846.pdf (accessed 7 February 2019).

Directive (EU) 2018/843 of the European Parliament and of the Council, "The Fourth Anti-Money Laundering Directive" (AML4), 30 May 2018, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843 (accessed 7 February 2019).

Europol (2017) "From suspicion to action. Converting financial intelligence into greater operational impact", pp. 1–44, Luxembourg: Publications Office of the European Union.

Financial Conduct Authority (FCA) (2017) "FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings", *Press Releases*, 31 January 2017, available at: https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure (accessed 20 February 2019).

Gillespie, Tarleton (2014) "The relevance of algorithms", pp. 167–194 in Tarleton Gillespie, Pablo J. Boczkowski, and Kirsten A. Foot (eds) *Media Technologies: Essays on Communication, Materiality, and Society*. Cambridge, MA: MIT Press.

Grommé, Francisca (2016) "Provocation: Technology, resistance and surveillance in public space", *Environment and Planning D: Society and Space*, 34(6): 1007–1024.

Guba, Egon G. and Yvonne S. Lincoln (1989) *Fourth Generation Evaluation*. Newbury Park etc.: Sage.

Hammersley, Martyn and Paul Atkinson (2007) *Ethnography: Principles in Practice* (3rd ed). London & New York: Routledge.

Hildebrandt, Mireille and Antoinette Rouvroy (eds) (2011) *Law, Human Agency and Autonomic Computing. The Philosophy of Law Meets the Philosophy of Technology*. Oxon: Routledge.

HSC (Human Security Collective) and ECNL (European Center for Non-for-profit Law) (2018) "At the intersection of security and regulation. Understanding the drivers of 'de-risking' and the impact on civil society organizations", March 2018, pp. 1–106, available at: https://www.hscollective.org/wp-content/uploads/2018/05/Understanding-the-Drivers-of-De-Risking-and-the-Impact-on-Civil-Society-Organizations_1.pdf (accessed 7 February 2019).

Kaufmann, Mareile, Simon Egbert and Matthias Leese (2019) "Predictive Policing and the Politics of Patterns", *The British Journal of Criminology*, 59(3), 674–692.

Kitchin, Rob (2017) "Thinking critically about and researching algorithms", *Information, Communication & Society*, 20(1): 14–29.

Klumpenaar, Sjoerd (2015) "ABN Amro krijgt boete voor misstanden Dubai", *NRC Handelsblad*, 4 November 2015, available at: https://www.nrc.nl/nieuws/2015/11/04/abn-amro-krijgt-boete-voor-misstanden-dubai-a1411763 (accessed 8 February 2019).

Kroener, Inga and Daniel Neyland (2012) "New technologies, security and surveillance", pp. 141–148, in Kirstie Ball, Kevin D. Haggerty and David Lyon (eds) *Routledge Handbook of Surveillance Studies.* New York: Routledge.

Lagerwaard, Pieter (2015) "Negotiating global finance: Trading on Dalal Street, Mumbai", *Journal of Cultural Economy*, 8(5), 564–581.

Latour, Bruno (1992) "Where are the missing masses? The sociology of a few mundane artifacts", pp. 225–258 in Wiebe. E. Bijker and John Law (eds) *Shaping Technology/Building Society: Studies in Sociotechnical Change*. Cambridge, MA: MIT Press.

Latour, Bruno (1999) *Pandora's Hope. Essays on the Reality of Science Studies.* Cambridge, MA: Harvard University Press.

Latour, Bruno (2005) *Reassembling the Social. An Introduction to Actor-Network-Theory.* Oxford: Oxford University Press.

Lazar, Jonathan, Jinjuan Heidi Feng and Harry Hochheiser (2017) *Research Methods in Human-Computer Interaction* (2nd ed.). Cambridge, MA: Morgan Kaufmann.

Law, John and Evelyn Ruppert (2013) "The social life of methods: Devices", *Journal of Cultural Economy*, 6(3): 229–240.

Manheim, Jarol B., Richard C Rich, Lars Willnat, Craig Leonard Brians and James Babb (2012). *Empirical Political Analysis: An Introduction to Research Methods*. Harlow: Pearson

Marcus, George E. (1995) "Ethnography in/of the world system: The emergence of multi-sited ethnography", *Annual Review of Anthropology*, 24(1): 95–117.

Mol, Annemarie (2010) "Actor-network theory: Sensitive terms and enduring tensions", *Kölner Zeitschrift Für Soziologie Und Sozialpsychologie*. Sonderheft, 50: 253–269.

Neyland, Daniel (2018). *The Everyday Life of an Algorithm.* Open Access: Palgrave Macmillan, available at: https://doi.org/10.1007/978-3-030-00578-8

NVB (Nederlandse Vereniging van Banken) (2017) "Position paper. Tegengaan terrorismefinanciering kan effectiever", Committee on Finance, Dutch House of Representatives, The Hague, 7 February 2017, available at: https://www.nvb.nl/media/document/001335_tegengaan-terrorismefinanciering.pdf (accessed 7 February 2019).

O'Grady, Nathaniel (2015) "A politics of redeployment. Malleable technologies and the localisation of anticipatory calculation", pp. 72–86, in Louise Amoore and Volha Piotukh (eds) *Algorithmic Life: Calculative Devices in the Age of Big Data*. London and New York: Routledge.

OM (Openbaar Ministerie) (2018) "ING betaalt 775 miljoen vanwege ernstige nalatigheden bij voorkomen witwassen", *Openbaar Ministerie*, 4 September 2018, available on: https://www.om.nl/@103953/ing-betaalt-775/ (accessed 7 February 2019).

Sismondo, Sergio (2010) *An Introduction to Science and Technology Studies* (2nd ed.). Chichester, UK and Malden, MA: Wiley-Blackwell.

Suchman, Lucy A. (2007) *Human-Machine Reconfigurations: Plans and Situated Actions*. New York: Cambridge University Press.

Suchman, Lucy (2012) "Configuration", pp. 48–60 in Celia Lury and Nina Wakeford (eds) *Inventive Methods: The Happening of the Social*. Oxon and New York: Routledge.

Suchman, Lucy, Karolina Follis, and Jutta Weber (2017) "Tracking and targeting: Sociotechnologies of (in) security", *Science, Technology, & Human Values*, 42(6): 983–1002.

Van Veeren, Elspeth (2018) "Invisibility", pp. 196–200 in Roland Bleiker (ed.) *Visual Global Politics.* London and New York: Routledge.

Vayre, Jean-Sébastien (2018) "Comment décrire technologies d'apprentissage artificiel? Le cas des machine à prédire", *Réseaux*, 5(211): 69–104.

Verbeek, Peter-Paul and Adriaan Slob (eds) (2006) *User Behavior and Technology Development*. Dordrecht: Springer.

Weber, Jutta (2016) "Keep adding. On kill lists, drone warfare and the politics of databases", *Environment and Planning D: Society and Space*, 34(1): 107–125.

Wesseling, Mara and Marieke de Goede (2018). Beleid Bestrijding Terrorismefinanciering. Effectiviteit en Effecten (2013–2016). University of Amsterdam commissioned by The WODC (Research and Documentation Centre) of the Dutch Ministry of Justice and Security, Amsterdam, December 2018.

Ziewitz, Malte (2016) "Governing Algorithms: Myth, Mess, and Methods", *Science, Technology, & Human Values*, 41(1): 3–16.