Review of International Studies, page 1 of 19. doi:10.1017/S0260210517000353

RIS

The chain of security

Marieke de Goede*
Professor, Political Science, University of Amsterdam

Abstract

Increasingly, private companies – including Twitter, airlines, and banks – find themselves in the frontline of fighting terrorism and other security threats, because they are obliged to mine and expel suspicious transactions. This analytical work of companies forms part of a chain, whereby transactions data are analysed, collected, reported, shared, and eventually deployed as a basis for intervention by police and prosecution. This article develops the notion of the *Chain of Security* in order to conceptualise the ways in which security judgements are made across public/private domains and on the basis of commercial transactions. Drawing on the work of Bruno Latour, this article understands the security chain as the set of practices whereby commercial transactions are collected, stored, transferred, and analysed, in order to arrive at security facts. Understanding the trajectory of the suspicious transaction as a series of translations across professional domains draws attention to the processes of sequencing, movement, and referral in the production of security judgements. The article uses the chain of financial suspicious transactions reporting as example to show how this research 'thinking tool' can work. In doing so, it aims to contribute to debates at the intersection between International Relations (IR) and Science-and-Technology Studies (STS).

Keywords

Security Practice; Security Knowledge; Latour; Terrorism; Data; Finance

Introduction: Suspicious transactions

In current political debate and counterterrorism policy, we can signal a broad trend whereby security authorities require private companies to monitor transactions, report suspect statements, close accounts, and mine their databases for potential terrorist connections. In November 2014, for example, the report into the killing of UK soldier Lee Rigby suggested that Facebook may have been able to stop the attack, because one of the perpetrators had expressed his intentions to 'kill a soldier' in his online communications. The UK Intelligence and Security Committee (ISC) found that *if* this online exchange had been known to security services, the perpetrators might have been stopped. The report laments that Internet service providers like Facebook do not regard themselves to be under any obligation to report such suspicious expressions to authorities.[1] In response, Facebook did not question whether such security role would be within its legal competences, but instead revealed that

* Correspondence to: Marieke de Goede, Department of Political Science, University of Amsterdam, PO Box 15578, 1001NB Amsterdam, The Netherlands. Author's email: m.degoede@uva.nl

[1] Intelligence and Security Committee of Parliament, *Report on the Intelligence Relating to the Murder of Fusilier Lee Rigby* (London, 25 November 2014), p. 7, emphasis added. See {http://isc.independent.gov.uk/committee-reports/special-reports} accessed 30 August 2016. The same is argued in the UK Parliament, Home Affairs Select Committee, *Radicalisation: the Counter-Narrative and Identifying the Tipping Point*

it routinely deletes customer accounts on the basis of potential links to terrorism. In fact, after the Rigby murder, Facebook reported to the British GCHQ that it 'had disabled seven of [the perpetrator] accounts ahead of the killing, five of which had been flagged for links with terrorism'.[2] Far-reaching legislation that obliges social media companies to report suspicious exchanges is currently being debated in the UK, as well as other countries including the US.[3]

Ahead of formal legislation, the UK National Counter Terrorism Internet Referral Unit works closely with companies, and has effected the removal of over 160,000 'pieces of extremist and terrorist material' from the Internet.[4] By comparison, since its establishment in January 2015, Europol's Internet Referral Unit has removed more than 6,000 pieces of suspect online content, in cooperation with social media companies.[5] In February 2016, Twitter announced that on its own initiative it has suspended over 125,000 accounts in less than one year, primarily for potential links to IS (Islamic State in Iraq and the Levant). This may be new for Twitter, but it is not so for banks, wire transfer companies and other financial institutions, which have the legal obligation to report suspicious transactions potentially relating to terrorism in a regulatory regime dating back to the mid-1990s. In the UK for example, Suspicious Transactions Reports from the banking sector increased from over 200,000 in 2007 to over 300,000 in 2013.[6]

Transactions analysis forms part of a security *chain*, whereby commercial data are analysed, collected, reported, shared, moved, and eventually deployed as a basis for intervention by police and prosecution. In this context, private companies – including Facebook and Twitter, airlines and banks – find themselves in the frontline of fighting terrorism and other security threats. Companies identify, select, search, and interpret suspicious transactions. They monitor, regulate, restrict, and expel client groups. Clearly, this is not a new phenomenon: as a growing literature notes, private companies, in many ways, have become security actors in their own right.[7] Existing literature offers substantial

(London, 25 August 2016), for example pp. 13–14, available at: {http://www.publications.parliament.uk/pa/cm201617/cmselect/cmhaff/135/135.pdf} accessed 2 September 2016.

[2] Leo Kelion, 'Facebook Hosted Lee Rigby Death Chat Ahead of Soldier's Murder', *BBC News* (25 November 2014), available at: {http://www.bbc.com/news/technology-30199131} accessed 30 August 2016.

[3] UK Parliament, Home Affairs Select Committee, *Radicalisation: the Counter-Narrative and Identifying the Tipping Point* (London, 25 August 2016), available at: {http://www.publications.parliament.uk/pa/cm201617/cmselect/cmhaff/135/135.pdf} accessed 2 September 2016; HR3654, Combat Terrorist Use of Social Media Act of 2015, US Congress, available at: {https://www.congress.gov/bill/114th-congress/house-bill/3654/text} accessed 2 September 2016.

[4] UK Metropolitan Police, 'Report Terrorist and Extremist Material Online' (25 April 2016), available at: {http://news.met.police.uk/news/report-extremist-and-terrorist-material-online-160089} accessed 2 September 2016.

[5] Council of the European Union, 'Note', Brussels (13 May 2016), p. 7, available at: {http://statewatch.org/news/2016/may/eu-europol-ct-centre-report-8881-16.pdf} accessed 22 June 2016.

[6] UK National Crime Agency, *Suspicious Activity Reports (SARs) Annual Report 2013* (London, July 2013), p. 5.

[7] Rita Abrahamsen and Michael C. Williams, *Security Beyond the State* (Cambridge: Cambridge University Press, 2011); Louise Amoore, *The Politics of Possibility* (Durham, NC: Duke University Press, 2013); Claudia Aradau and Rens van Munster, *Politics of Catastrophe* (London: Routledge, 2011); Marijn Hoijtink, 'Capitalizing on emergence: the "new" civil security market in Europe', *Security Dialogue*, 45:5 (2014), pp. 458–75; Anna Leander, 'The paradoxical impunity of private military companies', *Security Dialogue*, 41:5 (2010), pp. 467–90; Luis Lobo-Guerrero, *Insuring Life: Value, Security and Risk* (London: Routledge, 2016); Tony Porter and Heather McKeen-Edwards, *Transnational Financial Associations and the Governance of Global Finance* (Abingdon: Routledge, 2013); Darshan Vigneswaran, 'The contours of disorder: Crime maps and territorial policing in South Africa', *Environment and Planning D: Society & Space*, 32:1 (2014), pp. 91–107.

critical analysis of security professionals and their modes of knowledge production, including technical artefacts and calculative practices.[8] Research on Private Military Companies (PMCs) has focused on the question whether security is 'outsourced' to private companies, or whether companies have become 'deputised' by law enforcement.[9] There is increasing recognition that the conceptual divide between public and private is fluid and contested.[10] Sometimes, then, these security practices are understood as emergent public/private assemblages.[11]

Compared to private military or security companies, however, banks, airlines, and social media companies are extremely *reluctant* security actors. Policy initiatives in the name of countering terrorism have positioned a diversity of non-security actors into the frontline, including for example teachers and medical staff.[12] In the case of banks and Twitter, the political and moral pressure that they police their servers and mine their transactions databases is in tension with their profit motive and their obligations of client confidentiality,[13] even if commercial objectives become sometimes grafted onto new security roles.[14] Rather than a mode of security 'outsourcing', this involves a process of authorisation and appropriation, whereby private companies like banks, money transfers businesses, and Twitter reluctantly learn to *see* the world through a security lens. These examples challenge the common idea of a military-security nexus, that supposes an alignment between commercial interests and security projects. The public/private relation here is one of friction, tension and contradiction.[15] This yields a set of questions that is slightly different from those normally posed within the literatures on private security: What happens when non-security private companies – such as banks, but also airlines and social media companies – are effectively authorised to make security judgements in the frontline of fighting terrorism? What are the processes whereby commercial data such as Facebook expressions and financial records become inscribed with suspicion, and reported, shared, or moved from private to public domains? What are the contradictions and tensions between

[8] Didier Bigo, 'Security and immigration: Toward a critique of the governmentality of unease', *Alternatives*, 27:1 (2002), pp. 63–92; Jef Huysmans, *The Politics of Insecurity: Fear, Migration and Asylum in the EU* (London: Routledge, 2006).

[9] Deborah Avant, *The Market for Force: the Consequences of Privatizing Security* (Cambridge: Cambridge University Press, 2005); Joakim Berndtsson and Christopher Kinsey (eds), *The Routledge Research Companion to Security Outsourcing* (London: Routledge, 2016).

[10] Joakim Berndtsson and Maria Stern, 'Private security and the public-private divide: Contested lines of distinction and modes of governance in the Stockholm-Arlanda Security Assemblage', *International Political Sociology*, 5:4 (2011), p. 408. Also Mark B. Salter, 'Governmentalities of an airport: Heterotopia and confession', *International Political Sociology*, 1:1 (2007), pp. 49–66; Peer Schouten, 'Security as controversy: Reassembling security at Amsterdam Airport', *Security Dialogue*, 45:1 (2014), pp. 23–42.

[11] Abrahamson and Williams, *Security Beyond the State*; Berndtsson and Stern, 'Private security and the public-private divide'; Nadine Voelkner, 'Managing pathogenic circulation: Human security and the migrant health assemblage in Thailand', *Security Dialogue*, 42:3 (2011), pp. 239–59.

[12] Marieke de Goede and Stephanie Simon, 'Governing future radicals in Europe', *Antipode*, 45:2 (2013), pp. 315–35; Charlotte Heath-Kelly, 'Algorithmic autoimunity in the NHS: Radicalisation in the clinic', *Security Dialogue*, 48:1 (2017), pp. 29–45; Francesco Ragazzi, 'Countering terrorism and radicalisation: Securitising social policy?', *Critical Social Policy*, 37:2 (2016), pp. 1–17.

[13] Gilles Favarel-Garrigues, Thierry Godefroy, and Pierre Lascoumes, 'Sentinels in the banking industry: Private actors and the fight against money laundering in France', *British Journal of Sociology*, 48:1 (2008), pp. 1–19; Kirstie Ball, Ana Canhoto, Elizabeth Daniel, Sally Dibb, Maureen Meadows, and Keith Spiller, *The Private Security State? Surveillance, Consumer Data and the War on Terror* (Copenhagen CBS Press, 2015).

[14] The notion of 'grafting on' is taken from Tanja Murray Li, 'Practices of assemblage and community forest management', *Economy & Society*, 36:2 (2007), pp. 263–93.

[15] Emmanuel-Pierre Guittet and Julien Jeandesboz, 'Security technologies', in Peter Burgess (ed.), *The Routledge Handbook of New Security Studies* (London: Routledge, 2010), pp. 235–7.

security objectives and commercial interests, and how does security become grafted onto commercial environments?

This article develops the notion of the *Chain of Security* in order to conceptualise the ways in which security judgements are made across public/private domains and on the basis of commercial transactions. For Bruno Latour, a 'chain of translation' is the set of practices whereby objects are identified, collected, registered, transferred, and interpreted in the context of scientific research and the production of scientific facts.[16] Appropriating Latour's concept, I argue that we can visualise the path of the suspicious transaction as a chain of translation, whereby commercial transactions are collected, stored, transferred, and analysed in order to arrive at security facts (including for example frozen assets, closed accounts, and court convictions). This conceptualisation shifts focus toward the trajectory of the suspicious transaction *itself*, to follow its modulations as its moves across public and private domains. In doing so, the article aims to contribute to debates at the intersection between International Relations (IR) and Science-and-Technology Studies (STS). The dialogue between STS and IR is offering productive new ways of theorising and researching the role materialities and 'things' in international politics.[17] These literatures offer rich resources for analysing the 'material dimensions of knowledge production'.[18] This article engages more deeply with the analytical instruments offered in the work of Latour and others. It seeks to foster a 'radically processual understanding of producing security'.[19] It offers a way to unpack the tempo-spatial distribution of expert practices: by understanding knowledge production not as a nebulous process, but as dependent upon relatively regulated sequences of interpretation and movement.[20]

Before going on to develop this argument, it is important to emphasise that private security judgements such as account closures and asset freezing can have major effects on individual lives and political freedom. Critical questions have been raised concerning the criteria underlying judgements to remove online content and close bank accounts, and the limited possibilities that citizens have to seek redress when wrongly targeted.[21] Though perhaps we could argue that having a Twitter or Facebook account is not a human right, one US court has now ruled that boarding an airplane is not a luxury but a life's necessity in contemporary society, which is marked by geographically dispersed families.[22] Research into suspicious transactions mining in banks, moreover, has shown that these regulations have limited the operational scope and freedom of humanitarian organisations in recent

[16] Bruno Latour, *Pandora's Hope: Essays on the Reality of Science Studies* (Cambridge, MA: Harvard University Press, 1999), pp. 24–79; also Bruno Latour, 'Why has critique run out of steam? From matters of fact to matters of concern', *Critical Inquiry*, 30: winter (2004), pp. 225–48; Annemarie Mol, *The Body Multiple: Ontology in Medical Practice* (Durham, NC: Duke University Press, 2002); John Law and Annemarie Mol (eds), *Complexities: Social Studies of Knowledge Practices* (Durham, NC: Duke University Press, 2002).

[17] Mark B. Salter (ed.), *Making Things International 1: Circuits and Motion* (Minneapolis: University of Minnesota Press, 2015).

[18] Jacqueline Best and William Walters, 'Forum: Actor-network theory', *International Political Sociology*, 7:3 (2013), p. 347.

[19] Holger Stritzel, 'Security, the translation', *Security Dialogue*, 42:4–5 (2011), p. 343.

[20] Christian Bueger, 'Making things known: Epistemic practices, the United Nations, and the translation of piracy', *International Political Sociology*, 9:1 (2015), p. 7.

[21] See, for example, Lucie Krahulcova, 'Europol's Internet Referral Unit Risks Harming Rights and Feeding Extremism', *Access Now* (17 June 2016), available at: {https://www.accessnow.org/europols-internet-referral-unit-risks-harming-rights-isolating-extremists/} accessed 22 June 2016.

[22] The United States District Court for the District of Oregon, *Latif v. Holder*, *Opinion and Order*, 24 June 2014. In this case the court held that there may be 'numerous reasons [for] needing to travel overseas quickly such as the birth of a child, the death of a loved one, a business opportunity, or a religious obligation', p. 26, available

years.[23] We now also have examples whereby such banking requirements have led to the debanking of entire groups – disproportionally Muslim charities.[24]

More than a conceptual exercise, then, this article seeks to develop what Anna Leander calls a 'thinking tool', to empirically analyse and critique the ways in which companies act in the frontline of security practice. Thinking tools help to define 'what to think about' (the reluctant security practices of companies) and 'what to look at' (the concrete trajectory of the suspicious transaction).[25] The article starts with a discussion of Latour's work in order to examine how it is relevant to the study of security knowledge. It then goes on to follow a specific financial transaction, in order to illustrate a chain of security in practice. The final section of the article draws out how the concept of the chain of security seek to contribute to debates at the intersection of International Relations and Science-and-Technology Studies.

The chain of translation

In *Pandora's Hope*, Latour discusses and analyses the scientific practices that 'produce information about a state of affairs'.[26] In particular, he examines how scientific facts are produced in a research project concerning the question whether the Amazonian forest is advancing or retreating, which has great significance for our knowledge concerning climate change, as well as for possible investment opportunities in the local area. In order to reconstruct how scientists produce knowledge concerning the state of the Amazonian forest, Latour joins a field trip of French and Brazilian scientists, which has the objective to study the boundary between forest and savannah, and to collect soil samples for analysis. Latour offers a thick description of the soil science expedition, narrating how specific samples of soil are identified, collected, made transportable, inscribed in field logs and dossiers, transported to the (Parisian) 'center of calculation', analysed, debated and modelled, to produce, eventually, scientific facts as published in an academic journal. The process involves the 'passage from a clump of earth to a sign' to a scientific fact.[27]

The production of these pedological facts involves, for Latour, neither a flawless correspondence between the world and the word, nor a profound, unbridgeable gap of representation.[28] Instead, the

at: {https://www.aclu.org/sites/default/files/assets/no_fly_list_ruling__-_latif_v._holder_-_6-24-14.pdf} accessed 26 August 2016.

[23] See, for example, L. Boon-kuo, B. Hayes, V. Sentas, and G. Sullivan, *Building Peace in Permanent War: Terrorist Listing and Conflict Transformation* (London: International State Crime Initiative, 2015).

[24] Tom Keatinge, *Uncharitable Behaviour* (London: Demos, 2014); Tracy Durner and Liat Shretret, *Understanding Bank Derisking and its Effects Financial Exclusion* (Washington: Global Center on Cooperative Security, November 2015).

[25] Anna Leander, 'Thinking tools', in Audie Klotz and Deepa Prakash (eds), *Qualitative Methods in International Relations* (Basingstoke: Palgrave, 2008), p. 15.

[26] Latour, *Pandora's Hope*, pp. 24–79.

[27] Ibid., p. 51.

[28] The relation between materiality and representation is debated in a vast literature within International Studies, including, for example, David Campbell, 'International engagements: the politics of North American International Relations theory', *Political Theory*, 29:3 (2001), pp. 432–48; Michael J. Shapiro and Hayward R. Alker (eds), *Challenging Boundaries: Global Flows, Territorial Identities* (Minneapolis: University of Minnesota Press, 1996); Maja Zehfuss, *Constructivism in International Relations: the Politics of Reality* (Cambridge: Cambridge University Press, 2002); Jutta Weldes, *Constructing National Interests: The United States and the Cuban Missile Crisis* (Minneapolis: University of Minnesota Press, 1999). See also the Special Issue of *Review of International Studies*, 26:1 (2000).

translation of the world into words involves the *practice* of what Latour calls *circulating reference*. Each sequence in the process refers back to a prior object; each step of selection and inscription form the basis of the next move of the scientists. It involves countless little judgements along the way: selecting locations, collecting the earth, devising durable modes of inscription, coding the samples. This chain of reference, then, does not involve iron-clad scientific discovery but entails a 'risky, intermediary pathway' from situated clump of earth to pedological, scientific fact.[29] Or, as Latour put it in a different formulation, 'Accurate facts are hard to come by, and the harder they are, the more they entail some costly equipment, a longer set of mediations, more delicate proofs.'[30] At each link in the chain of soil collection, transportation, sampling and analysis, there are gaps as well as continuities. Rather than a rigid process, Latour understands the chain of translation to be a dynamic process of continuous circulation, referral, and contestation. It entails a movement 'back and forth', across many small gaps of understanding, connecting the two extremities of local matter and (scientific) fact.[31]

I argue that it is fruitful to redeploy Latour's concepts and methods in order to study the passage of a transaction from simple digital registration to a sign of suspicion to (possible) evidence of wrong-doing in the sphere of security. If we liken a transaction to the soil sample in the Latourian schema, we can render visible the practices that transform – for example – a financial record from simple bank registration, to suspicious transaction to (in some cases) court evidence. As in Latour's chain of soil analysis, translation is key to the movement and sequencing of transactions data across the security chain.[32] When transactions are reported from one professional domain to another, they are not simply *moved* but also *modified*: they acquire new meanings, new combinations with other data, and new capabilities. As Holger Stritzel has put it, 'translation … does not just "transport" meaning, but also creatively *produces* it, it rewrites, rearticulates, re-represents something in new terms'.[33] At each link in this security chain, then, a transaction does not just change in institutional context, but it changes in meaning: the significance it is inscribed with and the work it is able to do.[34] For example, within banking practice, a financial transaction may function as indicator of suspicion; within a Financial Intelligence Unit (FIU), the same transaction may function to help build typologies of risky financial patterns; whereas within a court of law it will have to function as evidence (of, for example, the pivotal position of the accused within a wider network).

Latour's approach has been taken up by existing literatures in security studies that have analysed security expertise as a 'chain of associations', or a 'chain of transcriptions'.[35] As Julien Jeandesboz

[29] Latour, *Pandora's Hope*, p. 40.

[30] Bruno Latour, 'From realpolitik to dingpolitik', in Bruno Latour and Peter Weibel (eds), *Making Things Public: Atmospheres of Democracy* (Cambridge, MA: MIT Press, 2005), p. 21.

[31] Latour, *Pandora's Hope*, p. 70.

[32] Barry, 'The translation zone'; Holger Stritzel, 'Security, the translation', *Security Dialogue*, 42:4–5 (2011), pp. 343–55; Holger Stritzel, 'Security as translation: Threats, discourse and the politics of localisation', *Review of International Studies*, 37:5 (2011), pp. 2491–517; Andreas Langenohl, 'Scenes of encounter: a translational approach to travelling concepts in the study of culture', in Doris Bachmann-Medick (ed.), *The Trans/National Study of Culture* (Berlin: Walter de Gruyter, 2014), pp. 93–118.

[33] Stritzel, 'Security, the translation', p. 344, emphasis in original; Barry, 'The translation zone', p. 414.

[34] Helen Nissenbaum, 'Privacy as contextual integrity', *Washington Law Review*, 79 (2004), pp. 119–58.

[35] Julien Jeandesboz, 'Smartening border security in the European Union: an associational enquiry', *Security Dialogue*, 47:4 (2016), p. 300; Gil Eyal and Grace Pok, 'What is security expertise? From the sociology of professions to the analysis of networks of expertise', in Trine Villumsen Berling and Christian Bueger (eds), *Security Expertise: Practice, Power and Responsibility* (London: Routledge, 2015), p. 53; Tony Porter, 'Tracing associations in global finance', *International Political Sociology*, 3:7 (2013), pp. 334–8.

has shown for example, the validity of the EU 'smart border' proposals was politically produced through a chain of associations whereby the smart border was successfully allied to particular technologies, industries, and databases. Mike Bourne and colleagues similarly analyse the development of security technologies as 'a succession of comings and goings' whereby laboratory processes 'reimagined, transposed and improvised' security aims.[36]

In our case, we face a number of stumbling blocks and challenges when redeploying Latour's concept of the chain of translation to the realm of security transactions analysis. A digitally recorded transaction (an ATM withdrawal, a Facebook expression, or a Passenger Name Record) is not material in the sense of the Amazonian soil. If Latour was able to follow the soil samples as they made their way, quite literally, from the depths of the Amazonian forest to Western European centres of calculation, the unpredictable trajectory of digital data is markedly less traceable. Digital transactions data can double, merge, and be endlessly copied. Data paths are fundamentally unpredictable. They hardly constitute the relatively static Amazonian soil samples, that remain securely preserved in their plastic bags and boxes as they move from forest to laboratory.

In addition, the production of security knowledge is far less regulated than that of scientific facts. Latour follows the process whereby the Amazonian expedition and soil collection leads to the eventual production of pedological facts in an academic publication. The production of scientific facts is tightly regulated through the professional conventions of soil scientists and related disciplines. Of course, we know from the literature in the history of sciences that such professional conventions are far from universal, and dependent on historical contingencies and the situated histories of scientists and their patrons.[37] Nevertheless, the contemporary production of scientific objectivity is tightly regulated and institutionally policed. The production of security knowledge, on the other hand, is much more *speculative*.[38] Expertise in the domain of terrorism and counterterrorism is profoundly disputed.[39] Routines for the production of security knowledge are not settled. These challenges are exacerbated by the prevalence of secrecy in the security domain.[40] In short, then, Latour's chain of pedological fact production seems relatively structured and certain compared to the messy, unpredictable, and secretive chains of translation underpinning security facts. As William Walters has put it, 'How do we "follow the actors" when they operate under cover of national security?'[41]

[36] Mike Bourne, Heather Johnson, and Debbie Lisle, 'Laboratizing the border: the production, translation and anticipation of security technologies', *Security Dialogue*, 46:4 (2015), pp. 307–25 Also, see for example, Deborah Cowen, *The Deadly Life of Logistics: Mapping Violence in Global Trade* (Minneapolis: University of Minnesota Press, 2014).

[37] Lorraine Daston and Peter Galison, 'The image of objectivity', *Representations*, 40 (1992), pp. 81–128; Steven Shapin, *A Social History of Truth: Civility and Science in Seventeenth-Century England* (Chicago: University of Chicago Press, 1994).

[38] Marieke de Goede, *Speculative Security: the Politics of Pursuing Terrorist Monies* (Minneapolis: University of Minnesota Press, 2012); Melinda Cooper, 'Pre-empting emergence: the biological turn in the War on Terror', *Theory, Culture & Society*, 23:4 (2006), pp. 113–35.

[39] Lisa Stampnitzky, *Disciplining Terror: How Experts Invented 'Terrorism'* (Cambridge: Cambridge University Press, 2013); Anna Leander, 'Technological agency in the co-constitution of legal expertise', *Leiden Journal of International Law*, 26:4 (2013), pp. 811–31; Sven Opitz and Ute Tellmann, 'Future emergencies: Temporal politics and law and economy', *Theory, Culture & Society*, 32:2 (2014), pp. 107–29.

[40] Oliver Belcher and Lauren Martin, 'Ethnographies of closed doors', *Area*, 45:4 (2013), pp. 403–10; William Walters, 'Drone strikes, dingpolitik and beyond', *Security Dialogue*, 45:2 (2014), pp. 101–18.

[41] Walters, 'Drone strikes, dingpolitik', p. 105.

However, I maintain that it is precisely in the context of the unsettled nature of security knowledge that appropriating and developing Latour's approach makes sense. Digital data are not materially bounded in the ways that drones, tanks, bodies, and boats are.[42] They are more akin to what Karen Knorr Cetina has called 'epistemic objects', which 'have the capacity to unfold indefinitely'.[43] Despite their 'lack of completeness', Knorr Cetina argues that epistemic objects *can* be subject to sociology of knowledge approaches, just as more traditional bounded things and tools are. In her argument, the incomplete, 'transient', and 'unfolding' ontology of epistemic objects, 'foregrounds the temporal structure'.[44] Knorr Cetina draws attention to the temporal, *processual* way through which unstable knowledge objects acquire 'stable thinghood'.[45]

The concept of the security chain takes up this challenge in relation to the epistemic object of the suspicious transaction, offering a way to unpack the temporal process through which it materialises. As with the Amazonian forest soil, data(sets) need to identified, selected, and cut from the continuous flow of worldly matter.[46] Data do not simply *flow* from one domain to another: they need to be rendered transportable, both technically and juridically. They need to be rendered recombinable with other technologies and datasets.[47] This involves complex juridical issues, concerning access, jurisdiction, and transfer. It also involves technical issues concerning the interoperability of systems and the complexity of technical integration of platforms, which is quite often more difficult than surveillance literatures might imply.[48] In addition, there is an increasing recognition that legal provisions like privacy and data protection do not strictly *restrain* data flows, but in fact *order* dataflows in particular ways and enable their materialisation.[49] In this sense, then, suspicious transactions data(sets) are akin Knorr Cetina's epistemic objects. In the chain of security, the suspicious transaction acquires a stabilised thinghood, which is coupled to the capacity to generate valid security action, including asset freezes and court convictions. It has become a security fact, underpinning policing judgements across public and private domains.

A security chain in action

I have argued that it is possible to visualise the trajectory of a suspicious transaction as a chain of translation. This approach attempts to develop thinking tools for a processual approach to analysing security knowledge. As a way of adding empirical depth to the notion of the security chain, this section hones in on the banking sector – before going on, in the next section, to draw out the

[42] All discussed in Salter, *Making Things International* (fn. 18)

[43] Karin Knorr Cetina, 'Objectual practice', in Theordore R. Schatzki, Karin Knorr Cetina, and Eike von Savigny (eds), *The Practice Turn in Contemporary Theory* (London: Routledge, 2001), p. 181.

[44] Knorr Cetina, 'Objectual practice', pp. 182–3.

[45] Ibid., p. 184.

[46] Urs Stäheli, 'Indexing: the politics of invisibility', *Environment and Planning D: Society & Space*, 34:1 (2016), pp. 14–29; Marilyn Strathern, 'Cutting the network', *The Journal of the Royal Anthropological Institute*, 2:3 (1996), pp. 517–35.

[47] Claudia Aradau and Tobias Blanke, 'The (Big) Data-security assemblage: Knowledge and critique', *Big Data & Society*, July–December (2015), p. 3; also Jutta Weber, 'Keep adding: On kill lists, drone warfare and the politics of databases', *Environment and Planning D: Society & Space*, 34:1 (2016), pp. 107–25.

[48] Rocco Bellanova and Gloria Gonzalez-Fuster, 'Politics of disappearance: Scanners and (unobserved) bodies as mediators of security practices', *International Political Sociology*, 7:2 (2013), 188–209.

[49] Rocco Bellanova and Denis Duez, 'A different view on the making of EU security', *European Foreign Affairs Review*, 17 (2012), pp. 109–214; Rocco Bellanova, 'Data protection, with love', *International Political Sociology*, 8:1 (2014), pp. 112–15; Paul de Hert and Serge Gutwirth, 'Privacy, data protection and law enforcement: Opacity of the individual and transparency of power', in Eric Claes, Antony Duff, and Serge Gutwirth (eds), *Privacy and the Criminal Law* (Oxford: Intersentia, 2006).

contribution of the security chain at the intersection between IR and STS. The banking sector is of particular interest, because banks' obligations to mine their databases, report suspicions, and freeze transactions is well established in law and regulation, and much further advanced than in other commercial sectors. Recent years have seen a substantial strengthening of what has been called 'financial warfare' or the 'weaponisation of finance'.[50] The broad policy aims within this complex regulatory landscape are to anticipate terrorist activities by analysing financial flows and to preempt suspicious money transfers. In this sense, financial warfare parallels current developments in the revolution in military affairs (RMA), which use risk-based strategies to deliver the (contested) promise of precision attacks.[51] But financial warfare is a very different type of 'war', operating not through bombs and guns, but through bureaucratic and relatively invisible practices of risk analysis.[52]

Substantial policy and regulatory activity has taken place in the domain of Counter-Terrorism Financing (CTF), ranging from the development of transnational compliance mechanisms by the Financial Action Task Force (FATF), to the implementation of financial sanctions list, to the adoption of new legal tools.[53]

If we really want to understand how the broad policy aims in the name of financial warfare *act* upon the world – for example, how they affect banks' procedures, impact upon client (groups), and lead to freezing decisions – we need a processual approach. Like Latour's Amazonian soil sample discussed in the first part of this article, financial transactions data have to be identified, collected, and made transportable. They need to be inscribed in dossiers, analysed, debated and modelled, in order to be rendered intelligible and valid as security facts. At each link in this chain of translation, this involves countless small judgements, and a 'dialectic of gain and loss'.[54] In other words, the financial transaction does not stay the same. It is (re)inscribed, (re)combined, modelled, and morphed.

In contrast to the security dream of following the money, I propose to *follow* the series of translations that render financial transactions into indicators of suspicion, into evidence of wrongdoing in the chain of security. In a schematic rendering, the chain looks roughly as in Figure 1. Banks and other financial institutions are required to deliver Unusual Transactions Reports relating to terrorism

[50] Elena Holodny, '2015 could be the year we witness the weaponisation of finance', *Business Insider* (5 January 2015); Zarate, *Treasury's War*.

[51] Mikkel V. Rasmussen, *The Risk Society at War* (Cambridge: Cambridge University Press, 2006); F Sauer and Niklas Schörnig, 'Killer drones: the silver bullet of democratic warfare?', *Security Dialogue*, 43:4 (2012), pp. 363–80.

[52] Mariana Valverde and Michael Mopas, 'Insecurity and the dream of targeted governance', in Wendy Larner and William Walters (eds), *Global Governmentality: Governing International Spaces* (London: Routledge, 2004).

[53] In Europe, the main legal parameter is the EU Fourth Money Laundering Directive (2015). For discussions of this regulatory domain, see Yee-Kuang Heng and Ken McDonagh, 'The other war on terror revealed: Global governmentality and the Financial Action Task Force campaign against terrorist financing', *Review of International Studies*, 34:3 (2008), pp. 553–73; Anthony Amicelle, 'Towards a new political economy of financial surveillance', *Security Dialogue*, 42:2 (2011), pp. 161–78; Valsamis Mitsilegas, 'Transatlantic counterterrorism cooperation and European values', in E. Fahey and D. Curtin (eds), *A Transatlantic Community of Law* (Cambridge: Cambridge University Press, 2014); Gavin Sullivan, 'Transnational legal assemblages and Global Security Law: Topologies and temporalities of the list', *Transnational Legal Theory*, 5:1 (2014), pp. 81–127.

[54] Latour, *Pandora's Hope*, p. 70.

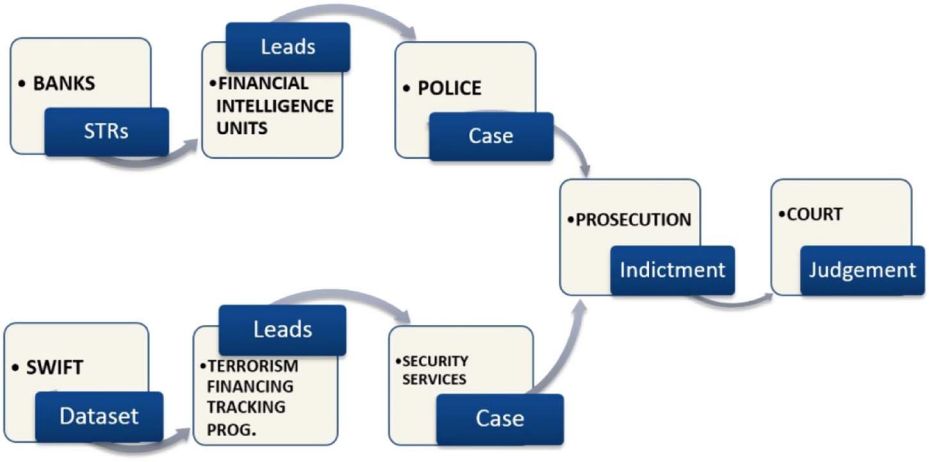

Figure 1. The security chain of financial transactions.

to their national Financial Intelligence Units (FIUs). FIUs develop leads for police and prosecution. Subsequently, cases may be referred for further investigation and court deliberation. Alternatively, cases may reach court through the so-called Terrorism Financing Tracking Programme (TFTP), the US-led security programme that analyses transactions data from SWIFT.

Mapping this process of translation, (re)inscription, gain and loss, captures the moments of politics. For example, European banks have started mining their databases for ATM transactions at the Turkish-Syria border.[55] These practices translate selected mundane transactions *from* routine ATM withdrawals *into* indicators of the potential travel of so-called foreign fighters en route to participate in the Syria conflict. In a further translation, such transactions may become indicators of terrorist intent before a court of law, especially now that European courts are increasingly faced with criminal prosecution of cases relating to travel to Syria and terrorist facilitation. In the remainder of this section, we will follow the life of a money transfer of €326 that an unnamed 28-year-old Dutch citizen sent via Western Union on to middle men in Turkey on 29 May 2014, who then handed it to the suspect's brother, Hatim R., who was known to be fighting for IS.[56] This transaction materialised as suspicious through the analytical work of Western Union, and it became reported, referred, modified, and recombined, to eventually form part of the court evidence that convicted the sender to a jail sentence for the financing of terrorism.

[55] Tom Keatinge, *Identifying Foreign Terrorist Fighters: The Role of Public-Private Partnership* (The Hague, International Center for Counterterrorism, 2015), p. 29; see also Thomson Reuters, 'Paris Attacks Showed Role of Small Transactions in Terror Finance; UN Meeting Hears' (15 April 2016), available at: {http://www.un.org/en/sc/ctc/docs/2016/thomson_reuters_15_april_2016.pdf} accessed 3 March 2017.

[56] This transaction is mentioned, alongside eight other transactions, in the Court Judgement that sentences the suspect for the financing of terrorism, *Judgement*, Court of Rotterdam, 15 March 2016, available at: {http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2016:1836} accessed 1 March 2017. Publicly available information from the Dutch National Bank reveals that in this particular court case, the transaction information was passed on from Western Union to the Dutch Financial Intelligence Unit to the Fraud Police (*Position Paper Dutch National Bank* [DNB]), Tweede Kamer (Dutch Parliament) (7 February 2017), available at: {https://www.tweedekamer.nl/kamerstukken/detail?id=2017D03625&did=2017D03625} accessed 3 March 2017.

Figure 2. From bank to FIU.

A first link in the chain (Figure 2) concerns banks and other financial institutions such as money transfer businesses. Banks are required by EU Directive *freeze* transactions relating to sanctions lists, and to *report* suspicious transactions to national Financial Intelligence Units. Suspicious Transactions Reports (STRs) have increased in number in recent years. In the UK for example, STRs increased from over 200,000 in 2007 to over 300,000 in 2013.[57] Banks face considerable challenges and uncertainties when implementing counterterrorism financing policies, including an uncertain and fragmented regulatory environment. They deploy a number of strategies to generate suspicious transactions, including in-house risk assessments, externally purchased software tools, and professional deliberation. Banks work with fine-grained client profiles and lifestyle analyses to identify abnormal and suspicious transactions.[58] Implications of bank profiling remain poorly understood. Client profiles can influence customer service and the cost of credit. In extreme cases, banks can terminate their business relationships with groups that are considered to be risky.[59] Another major challenge for banks is how to safeguard and practice privacy and client confidentiality, while meeting the substantial demands from regulators. Data protection directly affects the material architectures of data processing within the security chain.[60] In this sense, data protection does not simply restrain data flows, but *enables them* in specific ways. It regulates how data are concretely stored, handled, and shared.

Let us follow the €326 Western Union money transfer to Turkey, as it was translated from routine transfer to abnormal transaction. Western European financial institutions now scrutinise cash transfers, ATM transactions, and card spending within specific Turkish regions in order to identify potentially 'suspect travel' of persons en route to IS-held territories, as well as financial support to IS combatants. However, it is recognised that there are many legitimate reasons for bank transactions in this region, for example by military personnel stationed there and by diasporas' visiting family. Thus, compliance departments mine their transactions databases to filter on countries and regions, and combine the results with other information on bank accounts, loans, financial patterns, and social networks. The €326 sent by suspect X to unnamed persons in Turkey, resulted in one or more Unusual Transaction Reports filed by Western Union to the Dutch Financial Intelligence Unit, for a

[57] UK National Crime Agency, *Suspicious Activity Reports (SARs) Annual Report 2013* (London, July 2013), p. 5.

[58] Ball et al., *The Private Security State*?; Kevin Haggerty and Minas Samatas (eds), *Surveillance and Democracy* (Abingdon: Routledge, 2010); Mara Wesseling, 'The European Fight Against Terrorism Financing' (PhD thesis, University of Amsterdam, 2013).

[59] For example, the controversial decision by Barclays in 2013, when it closed the accounts of eighty businesses remitting money to Somalia without proof of abuse. As documented in the subsequent court case: *Dahabshiil Transfer Services Ltd v. Barclays Bank Plc*: High Court of Justice of England and Wales (EWHC) 3379, 2013.

[60] Bellanova and Duez, 'A different view'; Mireille Hildebrandt and Bert-Jaap Koops, 'The challenges of ambient law', *The Modern Law Review*, 73:3 (2010), pp. 428–60; Irma van der Ploeg, 'Biometrics and privacy', *Information, Communication & Society*, 6:1 (2003), pp. 85–104; Irma van der Ploeg and Govert Valkenburg, 'Materialities between security and privacy: a constructivist account of airport security scanners', *Security Dialogue*, 46:4 (2015), pp. 326–44.

Figure 3. From FIU to police / prosecution.

possible connection to terrorism financing. In other words, Western Union *translated* the €326 transaction from regular digital record of a money transfer, to an 'unusual' transaction in the sense defined by Dutch money laundering law (Wwft). The law prescribes that the identification of unusual transactions should depend upon subjective indicators to be determined by the financial institution, instead of criteria prescribed by the regulator. Money transfers constitute the largest proportion of reports received by the Dutch Financial Intelligence Unit in recent years.[61]

A second link (Figure 3) in the financial security chain concerns Financial Intelligence Units (FIUs), which are compulsory in all EU member states. FIUs receive Unusual Transactions Reports from banks, and in their turn pass on information to police and prosecutors (in the form of 'leads'). Very little is known about how FIUs handle, share, and analyse unusual transaction reports submitted by financial institutions. How do FIUs analyse and interpret banks' reports in order to develop police and prosecution leads? What types of in-house deliberation take place surrounding the prioritisation of investigations? Is the wire transfer to Somalia a legitimate support of family, or intended to aid al-Shahaab?

In order to start addressing these questions, let us further follow the life of the €326 wire transaction to Turkey in 2014. The Dutch FIU processed the unusual transaction report as one of 237,431 wire transfer transactions reported in 2014 of which an estimated 6 per cent was thought to be related to terrorism.[62] Within FIUs, the unusual transaction is made recombinable with other datasets as well as open source information, with a dual purpose. First, the FIU produces policing leads to be shared with national and regional police forces for follow-up investigations. Secondly, FIUs build their own databases of unusual transactions, which are used for secondary analysis to produce generalised suspicious data patterns and typologies. Such typologies and trends reports are important because they help define what comes to count as suspicious in the context of terrorism financing, and they can be used in criminal proceedings.

Our €326 abnormal transaction was subjected to further analysis by the Dutch FIU, which may typically involve a (re)combination of transaction information with information already on the national and international FIU databases. In further analytical steps, the abnormal transaction record will be combined with details from company registers, tax authorities, and – increasingly – publicly available information for example from social media sites like Facebook and Twitter. After analysis, our €326 was declared to be suspicious – which happened to an estimated 11 per cent of unusual transactions in 2014.[63] This translation from abnormal to suspicious fundamentally changes

[61] FIU-The Netherlands, *Annual Report 2014*, p. 21, available at: {https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/5276-fiu_jaaroverzicht_2014-engelsweb2.pdf} accessed 1 March 2017.

[62] FIU-The Netherlands, *Annual Report 2014*, pp. 21, 42, available at: {https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/5276-fiu_jaaroverzicht_2014-engelsweb2.pdf} accessed 1 March 2017.

[63] 29,382 transactions were declared suspicious of a total of 277,532 reports in 2014; see FIU-The Netherlands, *Annual Report* 2014, pp. 40, 21.

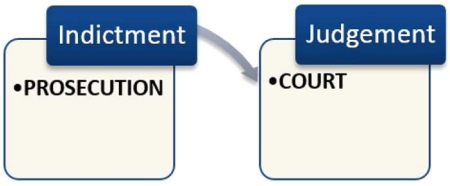

Figure 4. Court judgement.

the nature of the transaction: it now falls within a different data protection regime and can be shared with police forces, tax authorities, and fraud offices. It also gains significance in the context of terrorism financing typologies and social network analyses, as conducted by police and intelligence services. Information on this €326 transfer was shared with Dutch police and prosecution, who eventually arrested the sender.

A final link (Figure 4) in the chain of financial security concerns prosecution and courts. Clearly, most suspicious transactions reports generated in the financial security chain never lead to court cases. While limited in number however, terrorism financing court cases are interesting because they are at the forefront of the preventive turn in criminal law. They involve the criminalisation of facilitation and terrorist intent.[64] They bring potential violent futures into the present by criminalising ancillary acts of facilitation and financing. Financial transaction information may be brought before the court as evidence of terrorism facilitation and support. This was the case with our €326, which came to function as evidence before the court in the case of suspect X, accused of the financing of terrorism. In its sentence delivered in March 2016, the Rotterdam court mentions this specific transaction as evidence, alongside eight other money transfers made by the suspect, totaling €17,000. The court judgement asserts that the suspect intended the money to reach his brother Hatim, who is placed on the Dutch national terrorism list and who was convicted by the court of The Hague for participation in a terrorist organisation. The suspect was found guilty of multiple counts of the financing of terrorism, and of 'contributing to (increasing) destabilization and insecurity in (this region of) Syria'.[65] He was sentenced to 24 months imprisonment.

In a further and final translation, our €326 transaction is incorporated into a public narrative of a Dutch FIU 'success story'. It has become part of a sanitised narrative case example presented on the website of the Dutch FIU, serving to illustrate the 'life-pattern' of IS combatants.[66] In a position paper to Dutch Parliament in February 2017, this narrative was presented by the FIU as evidence of its successful combating of terrorism financing.[67]

[64] Marieke de Goede and Beatrice de Graaf, 'Sentencing risk: Temporality and precaution in terrorism trials', *International Political Sociology*, 7:3 (2013), pp. 313–31; Susanne Krasmann, 'Law's knowledge', *Theoretical Criminology*, 16:4 (2012), pp. 379–94; Jude McCulloch and Sharon Pickering, 'Precrime and counter-terrorism', *British Journal of Criminology*, 49:5 (2009), pp. 628–45; Lucia Zedner, 'Pre-crime and post-criminology?', *Theoretical Criminology*, 11:2 (2007), pp. 261–81.

[65] 'Een bijdrage geleverd aan de (verdergaande) destabilisering en onveiligheid in (de regio van) Syrië', *Judgement*, Court of Rotterdam, my translation.

[66] 'Levensonderhoud van een IS Medestrijder', available at: {https://www.fiu-nederland.nl/nl/levensonderhoud-van-een-is-medestrijder} accessed 14 June 2017.

[67] Position Paper Dutch National Bank (DNB), Tweede Kamer (Dutch Parliament) (7 February 2017), available at: {https://www.tweedekamer.nl/kamerstukken/detail?id=2017D03625&did=2017D03625}, accessed 3 March 2017.

Having followed, as example, the €326 transfer to Turkey, my suggestion is that we could similarly follow the life of a Passenger Name Record as it makes is way from commercial flight booking, to Advanced Passenger Information (API) security system, to deployment in front-line border policing, airport questioning, and possibly a denial of entry.[68] Alternatively, we could follow the life of a Twitter utterance, as it is flagged for violent content and reported to the new shared industry database designed to 'help identify potential terrorist content on social media and prevent its reappearance on other platforms'.[69] In a further translation, Twitter utterances may be recombined with other social media records to provide leads for police investigations, and to eventually constitute court evidence.[70] When we do, we will see that PNR data move quite differently across public and private spheres than financial or social media data do. Airline companies are required to share entire PNR datasets with security authorities – most notably the US Transport Security Agency (TSA) – in a system that 'pushes' data to other jurisdictions in advance of flight take-off.[71] Social media companies like Twitter, on the other hand, do not (yet) have the legal obligation to report suspicious accounts or utterances. However, they are increasingly cooperating with police, such as Europol's Internet Referral Unit, to identify and remove online content potentially related to terrorism.

In all these cases, the precise circulation of data between private companies and security authorities is slightly different, as is the mode of judgement concerning abnormalities and security risks. Nevertheless, the examples yield shared concerns about the locus of security judgements, the responsibilities of private companies, and the infrastructure of data-exchange. The notion of the chain of security can help address these concerns by mapping quite precisely how suspicious transactions materialise and enable security judgements. The purpose is not to suggest that this concept should *replace* other important analytical notions, like security expertise. Instead, the purpose is to add a possible thinking tool to the toolbox of materialist engagements with security studies.

At the intersection between STS and IR

Following the trajectory of a suspicious transaction as it materialises across the chain of security, I argue, offers a helpful thinking tool to analyse security expertise across public and private domains. I have illustrated this by following the life of a €326 transaction as it was translated from routine wire transfer to court evidence. This final section draws out how the notion of the chain of security aims to contribute to academic debates at the intersection between STS and IR. Specifically, it builds upon, and hopes to push forward, three strands of debate.

First, the approach focuses analytical attention on *practice* across public and private domains, but moves beyond the emphasis on background knowledge and routines in the literature that brings notions of practice to IR.[72] In this literature, practice is often understood as a 'routinised

[68] See also, Colin J. Bennett, 'What happens when you book and airline ticket? The collection and processing of passenger data post 9/11', in Elia Zureik and Mark B. Salter (eds), *Global Surveillance and Policing* (Devon: Willan Publishing, 2005), pp. 113–38.

[69] European Commission, 'EU Internet Forum: A Major Step forward in Curbing Terrorist Content on the Internet', Press Release, Brussels (8 December 2016), at: {http://europa.eu/rapid/press-release_IP-16-4328_en.htm} accessed 14 June 2017.

[70] Social media content, including, for example, Whatsapp messages, provide important evidentiary material in the criminal trials of people suspected of supporting IS.

[71] Amoore, *The Politics of Possibility*; Bellanova and Duez, 'A different view'.

[72] This literature is sometimes, but not exclusively, inspired by STS approaches. See Adler and Pouliot, *International Practices*; Rebecca Adler-Nissen, *Opting Out of the European Union* (Cambridge: Cambridge

type of behavior' through which actors 'create and maintain social orderliness'.[73] Routinisation depends on unspoken 'background knowledge'.[74] However, in contemporary security practice, background knowledge is often not settled. Regulation is relatively new and designed to remain flexible. Professionals are required by law to remain proactive, in order to anticipate the changing methods of potential terrorists. Companies like Twitter and banks have substantial discretion to make independent decisions on what they deem to be suspicious, and when to close accounts. They are encouraged by the regulator to deploy continually modulating and forward-looking strategies to identify suspicious transactions, accounts, or statements.[75] In this sense, security knowledge is often not settled, in the background, routine, and unspoken. Instead, it is formed in a situated and subjective manner, across public and private spheres.

Indeed, it is at the *point of practice* that regulation is given meaning and made to act upon the world.[76] As Annemarie Mol has argued in relation to health care, there is a difference between 'effective treatments' and 'treatment effects'.[77] The same may be said for policies: goals change and shift as the broad policy ambitions of counter terrorism are put into practice, generating unexpected interpretations, extensive professional efforts, and societal (side-)effects. This approach steers away from notions of habitus or hierarchies, whereby bureaucratic implementations become considered as driven by preconditioned professional outlooks or agendas.[78] Instead, it foregrounds the processual nature of knowledge formation, that – in the security realm – is understood as 'creative and constructive', rather than routine and 'habitual'.[79] It is not simply the case that (policy) ends are elusive, broadly formulated and malleable, it is also the case that ends do not necessarily 'drive action'. Instead, power is exercised when actors 'search for grip on situations'.[80] This is illustrated by our example of the €326, which materialises as suspicious when security actors search for grip on the complex political problem of so-called foreign fighters.

Second – and consequently – it is useful to distinguish between *knowledge* and *judgement* in order to grasp situated security decision-making beyond the routine. Security practices involve difficult, disputed, and deliberative judgements.[81] Decisions to report a transaction or freeze a money transfer are never fully automated, but generated through (re)iterative processes of datamining and deliberation. This

University Press, 2014); Bueger and Gadinger, 'The play of international practice'; Christian Bueger, 'Making things known: Epistemic practices, the United Nations, and the translation of piracy', *International Political Sociology*, 9:1 (2015), pp. 1–18; Iver B. Neumann, 'Returning practice to the linguistic turn', *Millennium*, 31:3 (2002), pp. 627–51; Mark B. Salter, 'Border security as practice: an agenda for research', *Security Dialogue*, 45:3 (2014), pp. 195–208.

[73] Bueger and Gadinger, 'The play of international practice', p. 451.

[74] Adler and Pouliot, *International Practices*, p. 16.

[75] See, for example, UK Treasury, *The Financial Challenge to Crime and Terrorism* (London, February, 2007).

[76] Knorr Cetina, 'Objectual practice', p. 175.

[77] Annemarie Mol, 'Proving or improving: On health care research as a form of self-reflection', *Qualitative Health Research*, 16:3 (2006), p. 406.

[78] Thomas Osborne, 'In defense of security', in Villumsen Berling and Bueger (eds), *Security Expertise*, pp. 60–75; Philip M. Frowd, 'The field of border control in Mauritania', *Security Dialogue*, 45:3 (2014), pp. 226–41.

[79] Knorr Cetina, 'Objectual practice', p. 175.

[80] Jesse Hoffman, 'Theorizing power in transition studies: the role of creativity and novel practices in structural change', *Policy Sciences*, 46:3 (2013), p. 26.

[81] Amoore and De Goede, 'Transactions after 9/11'; Jef Huysmans, 'What's in an act: On security speech acts and little security nothings', *Security Dialogue*, 42:4–5 (2011), p. 376; Bruno Magalhães, 'The politics of credibility: Assembling decisions on asylum applications in Brazil', *International Political Sociology*, 10:2 (2016), pp. 133–49.

involves an understanding of security judgements as dispersed and dependent on 'distributed agency'.[82] In a public statement for example, Twitter emphasised the complexity of judgements concerning identifying and closing terrorism-related accounts, and said: 'there is no "magic algorithm" for identifying terrorist content on the internet, so global online platforms are forced to make *challenging judgement calls* based on very limited information and guidance'.[83] As Anne Loeber has shown, professional policy implementation is best understood as a mode of *practical knowledge* where there is 'neither pre-set goal … nor … fixed and stable criteria by which to assess the correctness of a judgement'.[84] This is also the case with financial transactions reporting which, as we have seen in the previous section, encourages the deployment of flexible and subjective indicators.[85]

The concept of situated judgement as developed by Luc Boltanski and Laurent Thévenot is fruitful to capture and analyse the operations professionals perform and the moral claims they make when rendering judgement.[86] How do professionals classify a novel case within existing policy templates and orders of worth? What arguments of moral justification do they use when deciding to (not) report a transaction or (not) pursue a case? Boltanski and Thévenot have suggested that putting policy into practice is never a mechanistic following of a rule, but a subjective and situated process, with outcomes that vary. 'When one pays attention' to this moment, one sees much more than 'the application of a rule'. Instead, one sees an unchartered field of what they call 'situated judgement', understood as 'the confrontation between different forms of judgement expressed by the different actors implicated in the policy'.[87] The notion of situated judgement is a promising avenue to theorise the ways in which professionals classify concrete cases, appeal to rules and norms and enact the practical meaning of an overarching policy or principle. How do professionals analyse, deliberate, and decide on the normal, the abnormal and suspicious? How do they inscribe transactions with meaning, and how do they doubt, deliberate, and judge borderline cases?

An important element in this context is the *interface* between professionals and algorithmically-driven software systems that help them spot abnormalities.[88] It has been well documented that software technologies play an important role in suspect transactions analysis.[89] Algorithms have the

[82] Trine Villumsen Berling and Christian Bueger, 'Security expertise: an introduction', in Villumsen Berling and Bueger (eds), *Security Expertise*, p. 8.

[83] Twitter, 'Combating Violent Extremism' (5 February 2016), available at: {https://blog.twitter.com/2016/combating-violent-extremism} accessed 22 June 2016, emphasis added.

[84] Anne Loeber, 'Designing for Phronèsis: Experiences with transformative learning on sustainable development', *Critical Policy Analysis*, 1:4 (2007), p. 394.

[85] See also de Goede, *Speculative Security*, ch. 3.

[86] Luc Boltanski and Laurent Thévenot, 'The reality of moral expectations: a sociology of situated judgement', *Philosophical Explorations*, 3:3 (2000), pp. 208–231; also Frank Gadinger, 'On justification and critique: Luc Boltanski's pragmatic sociology and International Relations', *International Political Sociology*, 10:3 (2016), pp. 187–205; Julien Jeandesboz, 'Justifying control: EU border security and the shifting boundaries of political arrangement', in Raphael Bossong and Helena Carrapico (eds), *EU Borders and Shifting Internal Security* (Switzerland: Springer International, 2016), pp. 221–38.

[87] Boltanski and Thévenot, 'The reality of moral expectations', p. 216; also Loeber, 'Designing for Phronèsis'.

[88] Nathaniel O'Grady, 'Data, interface, security: Assembling technologies that govern the future', *Geoforum*, 64 (2015), pp. 130–7.

[89] Anthony Amicelle and Gilles Faravel-Garrigues, 'Financial surveillance: Who cares?', *Journal of Cultural Economy*, 5:1 (2012), pp. 105–214; Ball et al., *The Private Security State*; Ana Isabel Canhoto and James Backhouse, 'Profiling under conditions of ambiguity – an application in the financial services industry', *Journal of Retailing and Consumer Services*, 14 (2007), pp. 408–19; David Lyon, *Surveillance After September 11* (Cambridge: Polity Press, 2003).

capacity to analyse large digital datasets and identify abnormalities and deviant patterns. They increasingly 'create the conditions of possibility' for security knowledge.[90] However – and in contrast to the more sensational claims in the literature – algorithms do not deliver fully automated security judgements. They need instructions concerning risk appetites, patterns, and thresholds. Furthermore, software systems are integrated into wider professional environments, leading to processes of appropriation that are situated and to some extent unpredictable.[91] Professional deliberations (often) take place about the significance and interpretation of algorithmically-generated 'red flags', and the right follow-up actions in terms of reporting or freezing. The production of security knowledge, in this sense, can be seen as an interplay between human and machine reading.[92] This approach steers away from grand claims concerning the independent agency of algorithms, in order to focus on what Louise Amoore and Volha Piotukh have called the 'little analytics'.[93]

Finally, the notion of the chain of security embraces Isabelle Stengers's search for a mode of critique that does not seek to 'denounce', but that, instead, seeks to 'think with' the processual way in which orders, identities, and facts become established.[94] Stengers invites us to 'follow' the contingent process that bring (scientific) orders into being, 'without either ratifying or denouncing them'.[95] She seeks to proceed with a certain reverence for the object she follows: so as to 'try to open' its 'established identity' for critical thinking.[96] In this vein, the thinking tool of the chain of security seeks to follow the sequenced process of referral and (re)iteration underpinning security facts (such as closed accounts, frozen transactions, and court sentences). In doing so, it seeks to *think with* professionals, using their own doubts, challenges, and hesitations as anchors of (public) critique.

Conclusion

This article has developed the notion of the chain of security as a thinking tool to analyse and critique the formation of security knowledge and judgement across public and private domains. The article followed the life of a €326 wire transfer to Turkey, in order to analyse the professional processes and dilemmas at each link in this chain. Clearly, a security chain is not always linear: chains may be recursive, bungled, even circular. However, with this example I have started to unpack the ways in which financial data(sets) are carved off, reported, shared, and combined, to enable security interventions. As I have argued, the promises of the concept of the security chain are conceptual, empirical, and normative. Conceptually, it moves the study of security knowledge beyond notions of the routine, in order to understand the creative and sequenced mode of security judgements across public and private spheres. Here, we come to understand security as a mode of

[90] O'Grady, 'Data, interface, security', p. 131, drawing on Manovich. See also Mike Annany, 'Towards an ethics of algorithms: Convening, observation, probability and timeliness', *Science, Technology and Human Values*, 41:1 (2016), pp. 93–117; also Amoore, *The Politics of Possibility*; Weber, 'Keep adding'.

[91] For example Anthony Amicelle and Elida Jacobsen, 'The cross-colonization of finance and security through lists: Banking policing in the UK and India', *Environment & Planning D: Society and Space*, 34:1 (2016), pp. 89–106.

[92] Katherine Hayles, *How We Think* (Chicago: University of Chicago Press, 2012).

[93] Louise Amoore and Volha Piotukh, 'Life beyond big data: Governing with little analytics', *Economy & Society*, 44:3 (2015), pp. 341–66.

[94] Isabelle Stengers, *The Invention of Modern Science* (Minneapolis: University of Minnesota Press, 2000), p. 15.

[95] Ibid., p. 69.

[96] Ibid., p. 15.

practical knowledge that is not purely or primarily driven by ostensible policy ends, but which exercises power at the point of practice. Empirically, the approach fosters long-term, ethnographic engagement with security professionals, which is often missing from current practice-based approaches to international studies.[97] Normatively, the approach takes seriously the modes of professional judgement at each link of the security chain: it seeks to critique without judging. It entails an agenda of critique that follows rather than denounces established categories.[98]

In The *Making of Law*, Latour reflects on the different ways in which scientific and legal knowledges are generated. Legal facts are generated through prolonged processes of 'hesitation and doubt', 'so as not to rush to blindingly obvious truths'. Scientific facts, on the other hand, require formulation and judgement through the strict procedures of a discipline. 'Impassioned scientists, having promoted their object as much as possible in their articles, leave it to history, … and thus to future scientists, to judge whether they were right or wrong in making a particular assumption.'[99] Different from law and science, security entails its own kind of knowledge, of a specific, unchartered kind. Security knowledge resonates with science, law, and finance. Yet security has a specific temporality oriented toward urgency and preemptive action.[100] This means that the practices of knowledge through which security claims are produced are less routine, and more speculative. In the field of security, perhaps even more than other practical fields, policies are controversy-driven and knowledge claims are continually contested. Following the life of the suspicious transaction across a chain of security translation promises to help analyse how security knowledge is claimed, generated, and (un)settled in practice.

Acknowledgements

Three anonymous readers for *Review of International Studies* are thanked for their critical comments, which helped strengthen this piece. The article greatly benefited from discussions with colleagues, including Louse Amoore, Rocco Bellanova, Luc Fransen, Marlies Glasius, John Grin, Beste Işleyen, Francisco Klauser, Polly Pallister-Wilkins, Sven Opitz, Darshan Vigneswaran, and colleagues of the *Transnational Configurations, Conflict and Governance Research* group. Special thanks to Annemarie Mol for her support of this project. Pieter Lagerwaard provided research assistance. This article is part of the European Research Council project: *FOLLOW: Following the Money from Transaction to Trial* (ERC-2015-CoG 682317).

Biographical information

Marieke de Goede is Professor of Political Science at the University of Amsterdam. Her research focuses on the politics of countering terrorism, financial intelligence and the role of banks in security

[97] This point is made in S. Abrahamsson, F. Bertoni, R. Ibanez, and A. Mol, 'Living with Omega 3: New materialism and enduring concerns', *Environment and Planning D: Society & Space*, 33:1 (2015), pp. 4–19; but see for example, Laurent Bonelli and Francisco Ragazzi, 'Low-tech security: Files, notes and memos as technologies of anticipation', *Security Dialogue*, 45:5 (2014), pp. 476–9; Rivke Jaffe, 'The hybrid state: Crime and citizenship in urban Jamaica', *American Ethnologist*, 40:4 (2013), pp. 734–48; Mark B. Salter, 'Expertise in the aviation security field', in Mark B. Salter and Can E. Mutlu (eds), *Research Methods in Critical Security Studies* (New York: Routledge, 2013).

[98] Stengers, *The Invention of Modern Science*, p. 15; see also, for example, Louise Amoore, 'Security and the incalculable', *Security Dialogue*, 45:5 (2014), pp. 423–39.

[99] Bruno Latour, *The Making of Law*, trans. Marina Brilman and Alain Pottage (Cambridge: Polity, 2010), quotes taken from pp. 220, 225, and 209, respectively.

[100] Opitz and Tellmann, 'Future emergencies'.

practices. She is Principal Investigator of the ERC-funded project *FOLLOW: Following the Money from Transaction to Trial*. De Goede is author of *Speculative Security: the Politics of Pursuing Terrorist Monies* (University of Minnesota Press, 2012) and co-editor of the Special Issue on 'The politics of the list: Law security, technology', *Environment and Planning D: Society and Space* (34: 1). She is Associate Editor of *Security Dialogue*.