Article

SECURITY DIALOGUE

Security Dialogue
2014, Vol. 45(1) 23–42

DOI: 10.1177/0967010613515014
sdi.sagepub.com
SAGE

Security as controversy: Reassembling security at Amsterdam Airport

Peer Schouten
School of Global Studies, University of Gothenburg, Sweden

Abstract

Critical approaches to security have come to define themselves against mainstream security studies by not a priori assuming what security is, but rather taking it as an 'essentially contested concept'. Yet, as evidenced by the way in which recent 'turns' in the field have played out in the debate around airport security, ontological assumptions about security tend to restrict the scope of empirical analysis, with airport security being studied as, for instance, either discourse or practice. This article aims to propose an alternative methodological approach to security by studying security as controversy. Studying security as controversy means refraining from making a priori assumptions about the ontology of (in)security, instead considering it as itself at stake in – and hence the outcome of – security governance efforts. The article elaborates on this approach by drawing on core insights from actor-network theory, a conceptual and methodological toolkit that allows, as I show, a focus on how security actors perform security by enrolling, assembling and translating heterogeneous elements into stable assemblages that can be presented as definitive security solutions or threats. The article illustrates this approach through a look at the case of airport security at Amsterdam Airport in the aftermath of the 2009 Christmas terrorist attempt.

Keywords

actor-network theory, airport security, Amsterdam Airport Schiphol, controversy mapping, critical security studies, materiality, methodology, ontological politics, securitization, terrorism

Introduction

Air transportation has come to represent a driving force behind globalization, contributing $2.2 trillion to the global economy in 2012 alone (Air Transport Action Group (ATAG), 2012: 2). Airports make up central nodes in the critical infrastructure of globalization, where the circulation of high quantities of goods, persons and capital are managed. Since 9/11, terrorism has turned their security into a global controversy. Airport security has become a central preoccupation of security practitioners worldwide – governments spend billions yearly funding research on

Corresponding author:
Peer Schouten.
Email: peer.schouten@globalstudies.gu.se

explosive liquids, screening technologies and psychological guarding techniques. We are witnessing (note Lippert and O'Connor, 2003: 331) a 'radical shift in the way security … at airports and elsewhere in society [is] managed'. Thus, besides being a hallmark of economic globalization, airports are also sites where the contemporary preoccupation with security and risk is highly concentrated. Innovations in airport security governance are at the forefront of broader moves away from traditional forms of security governance planned and executed by the state, towards more hybrid and dynamic arrangements cross-cutting many of the divides that traditionally structure security studies (Salter, 2008b: xiv).

This makes airport security the focal point of a burgeoning subject literature (e.g. Adey, 2009; Berndtsson and Stern, 2011; Lippert and O'Connor, 2003; Salter, 2008b), reflecting broader debates on the 'stuff' of security (see Aradau et al., 2014; Salter and Mutlu, 2012). A variety of foci can be found in this debate, with airport security being studied, for instance, through the prism of discourse (Salter, 2008c); as expert practice (Salter, 2008a); or as socially constructed (Aas et al., 2009: 267). The point of departure for this article is the recent emergence of another approach to security – the 'material turn' – proponents of which argue that existing approaches, in prioritizing *human* security actors, fail to represent the full complexity of contemporary security governance. Airports often figure as an example, most visibly articulating both an increasing reliance on technologies in security provision and the fact that transnational security governance revolves more and more around object-centred controversies (Adey et al., 2011; Barry, 2012: 328–329; Neyland, 2009: 22), something reflected in the increasing securitization of such mundane things as letters, water bottles and scissors at airports (Aas et al., 2009; Neyland, 2009). As one recent contribution to the literature argues, at the airport, 'what are being socially sorted are not just data but also real bodies and things' (Jones, 2009: 85). The unfolding material turn in international relations[1] tries to analytically apprehend these observations, translating them into a more symmetrical reading of airport security, in which technological and social elements are approached on the same footing (Aradau et al., 2014; Bellanova and Fuster, 2013). This novel focus on materiality is most welcome, because critical approaches to security had hitherto come to define themselves against 'materialist' mainstream approaches on ontological grounds, emphasizing the cultural, linguistic and discursive constructedness of security (Marres and Lezaun, 2011: 490; see also Aradau, 2010; Coole and Frost, 2010: 3).

In this article, however, I want to suggest that the tendency of these successive turns in critical approaches to airport security to base themselves on an explicit ontological focus potentially precludes much of precisely what makes airport security such a fascinating case: the ontological shifts security undergoes at the airport. This article aims to provide an original position within debates about the nature of security by considering security not analytically, but anthropologically, focusing on the practice of security governance as ongoing attempts to settle controversies over security arrangements – a process in which the ontology of security itself can become reassembled. In doing so, the article picks up on a set of observations about airport security governance that have received relatively little attention in debates within critical security studies, and amplifies them by building on insights from actor-network theory. A tangential observation made on the sidelines of advances in the airport security literature is that airport security is time and again 'in the making' (Klauser et al., 2008: 120), and that in this process the very ontology of airport security is at stake. Neyland (2009), for instance, analyses the 'ontological shifts' that mundane objects undergo in airport security governance. This article aims to take these observations one step further by arguing that, when it is in the making, security itself is ontologically unstable – something hitherto overlooked by critical studies of airport security that start their *explanans* with fixed ontological assumptions.

The present article places itself in conversation with recent contributions to this journal that have pointed out how much existing approaches to security are premised on ontological monism and hence fail to represent the complexity of contemporary security governance, and therefore call for approaches that deploy the full diversity of elements assembled in security arrangements (Adey and Anderson, 2012; Aradau, 2010; Huysmans, 2011). Yet different from these contributions, which emphasize how material and social elements coexist in security arrangements, this article purports that the balance between 'human', 'social' or 'discursive' elements, on the one hand, and 'technical', 'material' or 'infrastructural' ones, on the other, is itself at stake in, and the outcome of, security governance practices. This article suggests that actor-network theory – 'an empirical version of poststructuralism' (Law, 2009: 145) – can contribute to a further move away from ontological monism in security studies by opening a novel analytical focus, namely, the 'ontological politics' (Mol, 1998) that occur during the unfolding of security controversies over time. Actor-network theory allows analysing security governance as attempts to settle the ontology of airport security *as* a matter of discourse, practice, performance or technology, and renders those efforts visible as part of the *explanandum* to be described in accounts of airport security governance.

The article proceeds as follows. The next section introduces actor-network theory and shows how it allows us to describe and account for the complexity of airport security at the crucial moments when security apparatuses – afterwards seemingly totalizing and immobile – are unstable, undefined and under construction. It then proceeds to the case study, which traces in two acts how the controversy over airport security that flamed up at Amsterdam Airport in the wake of the terrorist attempt on 25 December 2009 opened and was subsequently closed. First, in the prelude, I introduce airport security at Amsterdam Airport as a 'black box', smoothly functioning as a conduit facilitating large flows of goods and people. In the first act, following the 2009 attempt by the 'Christmas bomber', myriad spokespersons enter stage and open the black box of airport security, turning it into a controversy composed of many unpredictable elements. In the second act, we follow a range of security practitioners as they attempt to settle the controversy over security at Amsterdam Airport. A new security technology is introduced – the body scanner – facilitating this process of reassembling security. In the conclusion, I sum up the contribution that analysing security as controversy can make to security studies.

Actor-network theory: Security in action

At its core, actor-network theory is a conceptual and methodological toolbox for mapping controversies (Venturini, 2010). Actor-network theory – also called 'material semiotics', 'sociology of translation', 'philosophical anthropology' or 'empirical philosophy' – aims at shedding light on questions of how the social is composed and breaks up again, by tracing how actors assemble heterogeneous networks – discursive, institutional, technological and material – trying to have them act as one (Latour, 1987: 172). The theory – associated with names like Bruno Latour, John Law and Michel Callon – defines itself against classical sociology by approaching governance not in terms of stable social structures or the interaction of a limited set of pre-given actors, but rather as a perpetual struggle of competing efforts at stabilizing controversies in networks of actors (Kendall, 2004). In consequence, a core scholarly task becomes mapping controversies by following them through networks extending across space and time – in the process partially revealing the structure, dynamics and contingency of such governance networks as they present themselves to participants. Sociologists of science first introduced this approach in the late 1970s, when they shifted the focus from scientific knowledge as a stable entity 'out there' to 'science in action', to show that science

does not concern the discovery of pre-existing truths, but rather 'the outcome(s) or closure(s) of a controversy' (Barry, 2012: 326; see also Engelhardt and Caplan, 1989).

While mapping controversies hardly exhausts the resonance of actor-network theory in the social sciences, it is increasingly starting to adopt a life of its own as a methodological approach. For one, Latour leads a project called MACOSPOL (Mapping Controversies on Science for Politics) that aims to grant broad access to complex controversies.[2] Additionally, actor-network theory is increasingly deployed as a methodology for engaging social-scientific issues by 'opening up the black box' or 'mapping the controversy' surrounding a given concern. It is surprising that advocates of this approach have largely shunned the kind of subject matter of interest to security studies (see Barry, 2012: 334), and that, on the other hand, actor-network theory is only sparsely explored in security studies.[3] This lack of cross-fertilization is especially surprising since the stance that underpins actor-network theory seems to fit critical approaches to security like a glove: actor-network theory specializes in studying controversies, while what sets *critical* security studies apart from the mainstream is the consensus that security is – or should be – an 'essentially contested concept' (see e.g. Baldwin, 1997; McSweeney, 1999; Smith, 1999) – in other words, a controversy.

At the risk of oversimplification, I want to suggest that there are two – only analytically separable – components to actor-network theory of particular relevance to critical studies of security: first, its insistence on *process* and instability over structure and stability; which results, second, in its relational ontology and post-Cartesian *symmetry* between people and things, discourse and materiality, the social and technology, and, finally, controversies in human and natural sciences (Mayer, 2012b). Where the emergent 'material turn' in international relations largely explores the symmetry aspect of actor-network theory,[4] this article foregrounds the first of these two aspects: it illustrates the contribution that actor-network theory can make to security studies by turning the theory's process-oriented gaze towards security, by mapping the way security undergoes ontological shifts as part of unfolding controversies that make up the 'life' of airport security governance arrangements (Adey and Anderson, 2012). Echoing American pragmatists, I define controversies as the unfolding 'moments' in which issues arise that are resistant to settlement by extant apparatus, and in which diverse groups struggle to authoritatively establish arrangements that stabilize understandings of these issues, enact publics concerned and foreground relevant measures – moments at which the very ontologies of the entities involved are at stake (see Marres, 2007). Accordingly, the take on actor-network theory in this article has some resonance with the 'practice turn' in international relations, as it amounts to a closer focus on understanding security in practice rather than attempting to understand security in the light of a pre-given ontological understanding of what security means (see Bueger, 2013). Yet the crucial difference is that where practice approaches tend to focus on routinized security practices (Adler and Pouliot, 2011: 6), I here propose to look at security during controversies – that is, moments when security practices are arguably anything but routinized.

Mapping security controversies is best elucidated by contrasting it with studies of the economy inspired by actor-network theory (see e.g. MacKenzie, 2006). These look at how such 'actors' as economic models, statistical tools and accounting techniques, rather than mapping a pre-given 'economy', actually bring it into being. They aim at moving away from normative statements surrounding the essence of the economy to studying 'economization' – that is, the processes through which actors try to stabilize the economy by assembling a range of discursive, practical and material elements. To phrase the matter differently, the 'economy' as such does not exist, but rather comprises a broad set of practices, processes and concerns – most of them controversial – the stabilization of which involves 'actors' across the human/non-human divide. In line with actor-network theory's process-philosophical underpinnings, change is immanent, whereas stability of

economic action and understandings requires explanation, explanation that probably involves accounts of the more durable, technical or material, entities – such as aggregate statistics and digital taxation systems – that allow the stability of economic objects and subjectivities. Turning this gaze towards security, it becomes possible to broaden the scope of what 'securitization' means (see Huysmans, 2011). Paraphrasing the felicitous formulation of Çalişkan and Callon (2009: 370), the study of securitization should involve investigating the processes through which collective behaviours, materials and spheres of activities are established as (in)secure (whether or not there is consensus about the content of such qualifications). The scope of inquiry encompasses all efforts to settle controversies surrounding what security is and how it should be organized. This ties back into the main point of this article: through a conception of the ontology of security as the unstable product of controversies, the focus of study shifts towards the life of security arrangements and the unfolding of security controversies over time.

Mapping security controversies

So, how *does* one map controversies? Mapping controversies can be contrasted with Foucaultian archaeology:[5] like Foucault, actor-network theory destabilizes established (arti)facts by tracing them back to when they were still controversies; yet, as Foucault required an epistemological break with the present to unsettle common understandings, he was confined to studying the 'archive' (which is composed of texts). Actor-network theory, in short, makes it possible to turn this gaze towards the anthropological present (Law, 2009: 145–156; Pyyhtinen and Tamminen, 2011: 140). This brings it close to multi-sited ethnography's adage of 'follow the actors' (Latour, 2005: 68): mapping controversies entails tracing the associations made by actors that claim to speak for a network, by following them as they

> define and distribute roles, and mobilize or invent others to play these roles. Such roles may be social, political, technical, or bureaucratic in character; the objects that are mobilized to fill them are also heterogeneous and may take the form of people, organizations, machines, or scientific findings. (Law and Callon, 1988: 285)

In this way, I want to suggest, actor-network theory provides a toolbox with which to study 'a securitizing process that creates insecurities mainly through dispersing, through continuously associating, reassociating, tweaking and experimenting with materials, procedures, regulations, etc.' (Huysmans, 2011: 377).

Note how this differs from approaches that a priori focus on one ontological slice of security, such as, for instance, speech-act theoretical approaches to securitization (see, most explicitly, Vuori, 2008). In the approach proposed here, securitization is not an individualized and discursive act, but a collective process of performation (Bueger, 2013: 340), whereby agency is distributed over ontological divides (Mayer, 2012a). To emphasize how security controversies are just as much stabilized by discursive action as by non-human actors, it is useful to introduce actor-network theory's notion of 'actants'. In the most straightforward definition – from Oxford Dictionaries – an actant is 'a person, creature, or object playing any set of roles in a narrative'.[6] To paraphrase Mark Brown (2009: 167), from the perspective of security-in-the-making, human and non-human actants may be said to act insofar as security experts cannot yet predict what they will do. For example, the vast Icelandic ash cloud that burst into European airspace in 2011 was such a surprising actant: by disrupting complex socio-technical apparatuses of international air transport (Adey et al., 2011), it rendered the fragile security of mobile life visible. The notion of actant in actor-network theory is inspired by literary theory and radicalizes Aristotle's foregrounding of

action and plot over actors and characters in his *Poetics* (Barthes, 1975: 256–257; see also Bellanova and Fuster, 2013: 190–191; De Vries, 2007: 792): whether an object matters as an agent depends on the role it plays when it surfaces at a particular moment of a controversy. While actants like ash clouds can challenge established associations and thus engender controversy, actants can also be made to work together to end controversies. Actor-network theory uses the term 'black box' to refer to the singularity that arises when controversy, heterogeneity and productive agency are folded into a single, ontologically stable, entity (Bourne, 2012: 159). For instance, a diplomatic speech is only a felicitous diplomatic 'actant' if all domestic political disagreement is hidden in a 'black box' that the entire ministry may stand for (Neumann, 2007).

Importantly, actants do not necessarily speak for themselves. For ash clouds to become risks and terrorist networks security threats, they need to be qualified as such. Nor are security technologies such as screening machines and security guards straightforward security solutions: actor-network theory follows *spokespersons* that present us with how we should interpret these 'things' as actants rendering reality secure (see Beck and Kropp, 2010: 10–11; Latour, 1987: 70–73). Security is only tangible because of the discursive practices and material inscriptions that render it politically governable and analytically apprehensible. Those who claim to be in the business of providing security represent it by *other* things, which are then 'packaged' and 'sold' as containing threats or promoting security (Salter, 2008a: 258). These processes stabilize security controversies and render security tangible by translating it, for instance, through statistics, fences, border patrols and closed-circuit television (CCTV) systems. However, in contrast to studies focusing on security expertise as the defining element of security governance (e.g. Bigo, 2000; Klauser, 2009), controversy studies follows American pragmatism in insisting that participation is not restricted to experts; non-experts and concerned audiences can contest and influence expert claims (Barry, 2012: 326; Marres, 2007), and their voices – as articulated, for instance, in the media – should thus be mapped as part of the controversy. For the present analysis, this entailed a mixed ethnographic methodology comprising the 'interviewing' of a variety of human and textual spokespersons for the controversy over airport security. Concretely, the analysis followed the threat constituted by the 'Christmas bomber' as it travelled through, and underwent transformations in, different contexts, ranging from Dutch media to political and regulatory authorities, and from meetings in the Amsterdam Airport security control centre to technical reports on millimetre wave technology's capacity to render visible human bodies.[7]

The premise in assembling all these voices is that actors themselves provide us with rich material regarding who or what does or does not matter by transforming each other's statements into fact or fiction and by enrolling or demoting other actors (see Latour, 1987: 25, 202). This process, called 'translation', captures the literal transformation of elements through such associations made by actors. The concept of translation does not denote a neutral process, but rather 'all the negotiations, intrigues, calculations, acts of persuasion and violence thanks to which an actor or force takes, or causes to be conferred on itself, authority to speak or act on behalf of another actor or force' (Callon and Latour, 1981: 279). Translations are more than just new connections; they imply 'ontological shifts' in the elements reassembled in a controversy (Neyland, 2009: 26). Mol (1998) calls this 'ontological politics': contestation where the fundamental identities of actors, things and concerns are at stake. She emphasizes how, in principle, reality is multiple, to subsequently focus on the entanglements that produce and stabilize or disrupt dominant, incommensurable or overlapping ontologies. This process of translation concerns ontological *politics*, for establishing security *as* technical rather than social, or private rather than public, subsequently restricts and redefines accountability; distribution of scarce output; and/or the scope of possible action available to different affected actors. Rather than stable and pre-given, ontological categories and the assignment of agency to elements across them, become contingent accomplishments of security governance.

This approach displaces the focus from the ontology of security (what security is) towards the ways in which security becomes assembled, and thus from the definition of 'security' as a product to the 'acts' (Huysmans, 2011) of association and the resources mobilized to assemble and stabilize the various actants involved. Against the ontological 'turns' in security studies that reduce security to discourse, practice or materials, respectively, taking actor-network theory seriously implies 'ontological agnosticism': one cannot a priori decide which of these ontological 'slices' matter at all or matter most. It is only possible to show which mattered – how agency was assigned to them – in the unfolding of a specific controversy. While actor-network theory emerged out of the broader turn to practice in social studies of science, actor-network theory's relational premise (that anything can potentially matter but that nothing matters outside the associations through which it is constituted at any given moment – a core premise of classical American pragmatism, Whitehead's process philosophy and Prigogine's emphasis on 'becoming') can be understood to radicalize the emphasis that practice approaches to security place on 'security in action' as a departure from mainstream understandings of security (see Bueger and Villumsen, 2007). This profound commitment to relationality also explains why questions regarding Cartesian dualism or materiality are ultimately subsumed in actor-network theory under the task of apprehending how such categories are assembled and destabilized during the unfolding of controversies.

Assemblages versus apparatuses

What follows from our understanding of controversy and agnosticism towards the ontological nature of actants in security governance is that what matters is articulating the role of elements participating in controversies. This entails a slight reconceptualization of the concepts assemblage and apparatus, central notions in the airport security literature denoting how security governance at airports and elsewhere is performed not primarily by state security forces, but rather by networks of security actors that cross-cut public/private, local/global and formal/informal dichotomies (Lippert and O'Connor, 2003; Salter, 2008a, 2008b). The point of deploying these concepts has been to move away from the statist ontologies hitherto current in security studies, yet most studies using the term 'security assemblages' still predominantly focus on social interactions and discursive practices. While material elements are acknowledged as part of these arrangements, this is done in what Marres and Lezaun (2011: 494) call a 'sub-discursive' manner: security technologies are ontologically stable, only matter as conduits for discourse, and do not themselves form actants in, or the centre-point of, contestation (Valverde, 2011: 9).

Expanding recent proposals for more embodied understandings of security assemblages (Aradau, 2010; Aradau et al., 2014; Bourne, 2012; Huysmans, 2011; Voelkner, 2011), I define security *apparatus* as a set of 'socio-technical' arrangements that mediate relations and interactions within a specific sphere of activities, black-boxing some concerns and threats while foregrounding others (Beck and Kropp, 2010: 7; Feldman, 2011: 380). A security *assemblage* is the totality of relations structured by security apparatus, or the shifting – discursive, material, institutional, practical – 'milieu' upon which a security apparatus acts in order to render it secure (Foucault, 2007: 19–21, 37; Lippert and O'Connor, 2003: 333). By being a priori agnostic as to what elements apparatuses are made up of, actor-network theory grants materiality and non-discursive elements a more central role in the 'life' of security assemblages (Adey and Anderson, 2012). The notion of 'apparatus' is used precisely to articulate that security governance hinges on establishing 'systemic functional relationships between former incommensurables (humans and machines)' (Marcus and Saka, 2006: 105, cited in Aas, 2012: 7). To clarify, such entities as 'the aviation economy' and 'the shopping public' are assemblages contingent on socio-technical apparatuses composed of such actants as security scanners, managerial strategies, airplane technologies and biometric regimes, the

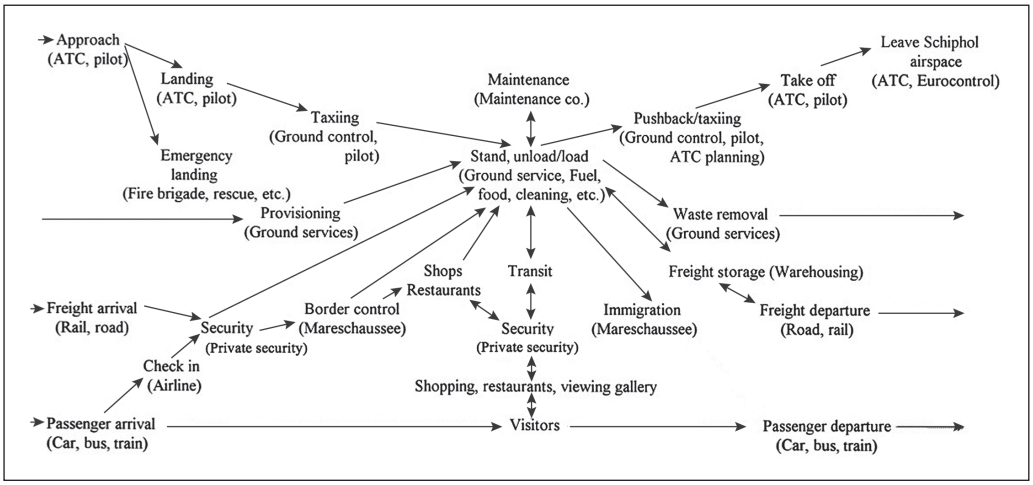

Figure 1. Functional flow diagram of airport activities and actors at Amsterdam Airport (adapted from Hale, 2001: 139).

workings of which form the focus of analysis inspired by actor-network theory. These apparatuses co-constitute and stabilize the assemblages that form their object of government by relaying controversy to more durable – often material or technical – entities (Schouten, 2013), yet the point of a sociology of controversies would be to emphasize that in controversies around their own functioning, apparatuses themselves become visible as assemblages requiring upholding.

In sum, these insights from actor-network theory lead to an understanding of airport security in which, on the one hand, the ontology of security is the *outcome* of controversy – and scholarly mappings thereof – and, on the other, the spokespersons for security – be they policy documents or public statements, the core object of study for critical discourse analysis – are only part of the 'actors' making up security apparatuses. The next section illustrates this understanding in the case of the controversy over airport security at Amsterdam Airport in the wake of the Christmas 2009 terrorist attempt.

Reassembling security at Amsterdam Airport

Prelude: Airport security as black box

Amsterdam Airport Schiphol (henceforth Schiphol) is a global hub airport, and an obligatory passage point for transatlantic travelers. With 51 million passengers in 2012, it ranks as the world's fourteenth-largest airport in terms of passenger throughput. With 80,000 people working at the airport, it supplies jobs to a number of people equal to 10% of the population of the Dutch capital Amsterdam (National Coordinator for Counterterrorism (NCC), 2006). Schiphol is a highly complex assemblage (see De Jong, 2012, and Figure 1) composed of 'coordinated but widely dispersed regulations, calculative arrangements, infrastructures and technical procedures' that render air transport governable (Mitchell, 2009: 409).

The security apparatus of Schiphol, bracketed in Figure 1, is equally complex. Over 10% of all private security personnel in the Netherlands work at the airport: 3500 private security guards, divided among the three biggest companies in the country (G4S, Securitas and Trigion), and a host of smaller, specialized companies. The bigger companies largely deliver operators of security technologies,

Table I. Organizations part of the Amsterdam Airport security apparatus.

Name	Acronym	Role
Private security companies		
Group 4 Securicor	G4S	Guarding/screening
Trigion	–	Guarding/screening
Securitas	–	Guarding/screening
International Security and Counter-Terrorism Academy	ISCA	Training (security awareness)
Pro-Check International	PCI	Security technologies, training (subsidiary of ICTS)
ICTS Europe	ICTS	Training (profiling)
Other security actors		
Airlines		Security check aircrafts
National Police		Patrolling
Customs		Screening goods
Royal Constabulary (Military Police)		Border control, overseeing
Regulatory authorities		
Schiphol Group security policy department		Regulation, overseeing, coordination; provides security infrastructure
National Coordinator for Counterterrorism	NCC	Overseeing, responsible for civil aviation security
Security and Public Safety Schiphol	BPVS	Governance platform
Ministry of Justice		Standard setting (National Civil Aviation Security Programme)
European Commission	EC	Standard setting (EC Regulation No. 300/2008)

Note: Compiled by author on the basis of Amsterdam Airport (2012).

while two of the smaller companies (Pro-Check International and the International Security and Counter-Terrorism Agency, ISCA) specialize in security awareness (Amsterdam Airport, 2012). The Royal Constabulary oversees airport security and, in turn, falls under the National Coordinator for Counterterrorism (NCC). Security is negotiated between all involved partners in a Platform ('Security and Public Safety Schiphol') that was set up as a response to terrorism, of which the goal is to reach an 'integrated approach' in which 'public and private partners make use of the same means and technology, each for its own specific goals and responsibilities' (NCC, 2006).

Besides these 'social' actors listed in Table 1, the apparatus also comprises a range of technologies, such as a CCTV surveillance system involving 1350 cameras; iris-recogition and other types of biometric scanners; over a hundred metal detectors; fences; and a range of other devices. Big private security companies (PSCs) – most notably G4S, Securitas and Trigion – are by and large responsible for security at the airport. Spokespersons for these PSCs insisted that the main reason for their dominance is their capacity to translate the fuzzy concept of security into key performance indicators (KPIs) that are said to represent what their security workforce and technologies do (see Lippert and O'Connor, 2003; Salter, 2008a); as one PSC manager indicated: 'each security indicator is translated into specific training modules that come with a specific task'.[8] When asked what security is, security managers were quick to dismiss security as 'vague' or 'a perception' – what mattered is how to render it visible, tangible and governable. To illustrate the key role security actors accord KPIs in constituting and weaving together security threats and solutions as apprehensible

actants in the Amsterdam Airport security apparatus, it is worth citing one senior PSC manager at length:

> Anyone can deliver a low-educated workforce, so in that sense we're incredibly expendable. Our expertise resides rather in the capacity of our management staff to be concrete…. The art in thinking is to ask how you can chop a general or abstract something into pieces, and how to make those pieces so concrete that someone who has to carry it out understands that if he does it in a certain way – and he can calculate that – that he's doing right…. Our KPIs do not just indicate the number of passengers screened, but also the number of mystery guests you've processed, the 100% presence rule, not causing any delays…. [This] makes our check into both a quantitative and a qualitative issue. If you add these qualitative performance indicators, a process gets a different character. More indicators per measured goal. An example: since Detroit, politics said, everything 100% check. Then I ask: what is 100% check? Undressing everyone? Emptying bags? Opening wallets in bags, too? Then five people at the airport say five different things. That doesn't work, so I want written on a piece of paper what we do. Not because I'm an idiot, but because the people that have to do it need to get a clear and uniform indication of A, B, C, D, and it has to be the same when I read it as when my client does. So if you talk about security measures, they always have to be translated concretely – both towards acting and intervening parties and clients. The art is how do you make cause and effect clear and coherent, keep them together. We're good within [name of company] at reducing all this to these very basic, tangible, explainable and measurable pieces.

Because KPIs embody both the object of airport security governance (measurable threats) and security solutions (measurable security outputs), they constitute key actants holding together the airport security apparatus. Another senior airport security manager explained that this was why airport security became privatized in 2003: 'one of the reasons was that, before, we couldn't make insightful what we actually did to make things secure. To our best knowledge, security was simply about doing your round of patrolling'. The privatization of security introduced KPIs so that everything related to security could be translated into numbers reproducible in statistics or on screens, or otherwise fit to 'govern at a distance'. In effect, KPIs are a conditio sine qua non – an 'obligatory passage point' in actor-network theory parlance – to have the dispersed actors that make up the airport security apparatus act as one. It is necessary to have abstract and mobile indicators of security, for 'airport security' needs to circulate between no less than 16 regulatory authorities involved at the airport, and KPIs allow the translation of security measures into data comparable to standards set by a host of far-flung actors, such as the European Union and the US Transport Security Administration (TSA) (Amsterdam Airport, 2007).

Act 1: Opening the Pandora's box of airport security

Until Christmas 2009, the global securitization of aviation had left Schiphol relatively untouched. Until then, in actor-network theory parlance, security was 'black boxed', forming part of the hinterland of the airport. Security operated as part of a bigger whole and was only visible in routine metal and baggage checks for travellers, and scarcely spoken about on websites or in the Dutch media. On Christmas Day 2009, the Nigerian Umar Farouk Abdulmutallab boarded flight Northwest 253 at Amsterdam Airport Schiphol with 80 grammes of the highly explosive chemical PETN strapped inside his trousers. As the airplane approached its final destination, Detroit, Umar attempted to ignite his bomb by injecting a chemical into the package (*Reuters*, 2009). While his attempt failed, Umar's action – coordinated with Al-Qaeda in Yemen – opened up a global controversy concerning not just security at Schiphol, but also, as it revealed the fragility of established security measures at airports worldwide, airport security more generally (Lipton and Shane, 2009).

The same complex security apparatus of over 3500 private security guards, CCTV systems, metal detectors, police officers and biometric scans that functioned smoothly as the hinterland of the airport before, now had people speaking for it in a different way. Newspapers worldwide acted as a confused array of worried spokespersons challenging the associations made at the airport; the Dutch National Coordinator for Counterterrorism asserted that the airport security apparatus 'met required regulations' (*NRC Handelsblad*, 2009a); and the Royal Constabulary wondered if the security measures really targeted terrorists or rather the continuity of airport retail.[9] Metal detectors were cast as useless, outdated scrap metal, unable to stop terrorists. As one newspaper put it: 'At this time, ICTS [an Israeli PSC based in the Netherlands] and the Dutch security firm G4S are hurling recriminations at each other, as are the authorities at Schiphol, the Federal Aviation Authority and U.S. intelligence officials' (Melman, 2010). Previously one of Europe's preferred airports, Schiphol was now represented as a 'terror airport' by the media (Van der Kloor, 2010) – an unwitting play of words on the literal meaning of Schiphol as 'ships hell' – and the previously 'clean' areas after the security checks now became potentially 'dirty' with prohibited liquids and gels. The black box of the airport security apparatus was opened, having become a Pandora's box of infinite elements, processes and relationships to be questioned, tested and improved. To make things worse, the media expanded the controversy from a relatively manageable expert concern into an imbroglio composed of a more diffuse set of issues, by tying it into larger controversies over privacy, terrorism and the privatization of security (see Bellanova and Fuster, 2013).

Act 2: Reassembling the apparatus of airport security

It had become imperative to put an end to this controversy, which threatened to demote Schiphol from its position as an obligatory transatlantic passage point: airlines could circumvent it by rerouting planes to other European airports, potentially resulting in large financial losses (Schiphol Group, 2011: 106). A few weeks after the terrorist attempt, the controversy settled around two issues. On the one hand, it concerned the private security guards working at the airport. Additionally, global media and airport security professionals attacked the scanning equipment in place. As Abdulmutallab had liquids on him, metal scanners – the prevalent technology at the time – would never have been sufficient.

Two alternative pathways thus emerged at the core of the controversy. If the problem was outdated technology, then perhaps a new, better scanner could be the actant to end the controversy (*New York Times*, 2009; *NRC Handelsblad*, 2009b) by assuring concerned stakeholders that potential bombs would be detected. If, however, the problem concerned bad guarding, then another actant – better 'security awareness' – could fulfil the same role and close the gap (Dahlkamp et al., 2010). The controversy clearly divided the different actors in the airport security apparatus. On the one hand, the airport concern and larger PSCs argued that reliable technology could address all concerns by detecting dangerous objects and disciplining the security guards; on the other, smaller, specialized PSCs and the NCC took that same workforce as 'human capital' that could be capitalized upon through security-awareness programmes. It was now up to Schiphol's security managers to attempt to settle the controversy by reassembling all these loose elements. In order to stabilize the assemblage, these unstable actants had to be enrolled into the security apparatus, or it had to be shown that they were not relevant at all – a nettlesome task, as the very ontology of (in)security was at stake in defining whether human error or technological failure had made the terrorist attempt possible (see Neyland, 2009: 26).

Belinda Kreugel, a former guard from the private security company G4S, challenged the role of guards within airport security. She argued that security guards are only trained to respond to the beeps emitted by metal detectors, instead of observing people's behaviour (Van den Dongen and

Olmer, 2009). Politicians and security professionals quickly picked up on the newspaper article in which Kreugel's comments appeared, entitled 'Critique of Useless Monitoring', to advance their own agendas. Particularly loud were the voices of two Israeli PSCs, ICTS (International Consultants on Targeted Security) and ISCA (International Security and Counter-Terrorism Academy), that operated at Schiphol. As the chief executive officer of ISCA explained:

> Guards at Amsterdam Airport that now spend eight hours a day looking at lights on metal detectors, can be the heroes of tomorrow. Now procedures and technologies are leading men, but we want men to lead both. In Israel, where security awareness is the standard approach to security, most incidents are actually stopped by simple guards, not by special forces. Why? Guards are always there – when you help them optimize their definition of behaviour and appearance that falls within the scope of the normal, they'll be able to … genuinely recognize abnormal behaviour. The idea is to endow each employee with a plan of attack.

He translated the hitherto dominant security technologies into a weakness ('tools can change, but intentions come first', he later added), while foregrounding his own expertise: under the header of 'security awareness', the Israeli PSC develops training programmes aimed at the 'human factor' of security. ISCA had already managed to enrol one powerful actor, the Dutch National Coordinator for Counterterrorism. As the latter's website puts it:

> Technology and security measures are only tools. They can never replace human beings in recognising terrorist or criminal activity. The NCTb therefore prioritises training in skills and knowledge aimed at recognising unusual or suspicious behaviour and taking action. The NCTb realises that security protection can be greatly improved … by strengthening security awareness. (NCC, 2009)

Countering concerns of those sceptical of low-wage security personnel shared by many at Schiphol (see below), ISCA's chief executive officer enrolls the airport security guards, of which 70% are second generation immigrants, as *especially good* security agents, as they share with Israelis the experience of living in unstable countries and are thus more prone to be security aware:

> Walking in the streets of a Moroccan capital, one has to be more aware of risks and deviant behaviour than in Amsterdam. The only thing that needs to change with these people is that now it is a distinct context that is defining what is acceptable and normal, and what not.[10]

While these arguments managed to enrol part of the security experts in the airport security assemblage – the NCC, the Royal Constabulary and even certain high-placed figures within the TSA (Ahlers, 2010) – security awareness has *not* become synonymous with airport security at Schiphol. Many more actants would have had to be convinced and enrolled to render security awareness more central to airport security.

Securitizing liquids

In order to explain why security awareness did not become the central solution to the airport security controversy, we have to return to the way in which security is inscribed, translated into abstract key performance indicators and communicated in this vast assemblage, involving over 5000 security professionals. KPIs consolidate the security apparatus of Schiphol by literally transforming all security elements – whether human, technical, singular or plural – into abstract and calculable objects of measurement, translating them from incongruent heterogeneity 'into matters about which it is possible to disagree' (Barry, 2012: 328; see also Salter, 2008a).[11] The centrality of KPIs to airport security explains why 'security awareness' did *not* become a central security solution.

Interviewees admitted that the 'security awareness' approach remains controversial, not only because Israeli profiling techniques are considered somewhat intrusive, but also because it has proven difficult to measure and compare the impact of security awareness. The NCC mandated the Dutch equivalent of the RAND Corporation to start researching the ways in which security awareness could be quantified and qualified.[12] If the NCC succeeds in the future in enrolling this powerful ally, it might be able to translate security awareness into the required KPIs and stabilize the controversy to its advantage. As a compromise, security awareness has become part of the basic training for all security personnel, which further includes compulsory knowledge of scanning equipment and the alarm number of the airport (Amsterdam Airport, 2010); however, the extensive programmes envisioned by the Israeli PSC ISCA have been put on hold.

So, what *did* become the central issue in the controversy over airport security? Before, only metals were securitized, and metal scanners enrolled as central actants providing protection; insecurity was translated into the possession of metal items that can be used as weapons. But, after the failed terrorist attempt of 2009, securitization shifted towards another class of objects. US media and Dutch airport security professionals pointed to new, unpredictable and dangerous actants that had to be dealt with in airport security apparatuses: liquids and powders. Abdulmutallab had (unsuccessfully) tried to use chemical powder and liquids – not knives or pistols – in his attempt to bring down the plane over Detroit. Hence, areas previously considered 'clean' in Schiphol security parlance (Amsterdam Airport, 2010) were now seen as possibly contaminated with dangerous objects. In this 'ontological shift' (Neyland, 2009: 26) during the controversy, securitization passed from human intentions towards dangerous bodies and objects attached to them.

Yet airport security authorities did not have to face dangerous liquids without a potential solution. After the terrorist attempt opened up the controversy over security at Schiphol, security managers added a new device to the apparatus for the production of security (paraphrasing Mitchell, 2009: 409). We see a new actant, the so-called body scanner, brought to stage, capable of rendering any object on the human body – liquid or not – visible on a screen. The device is based on millimetre wave back-scattered technology and makes it possible to assemble particular renderings of travellers' bodies into security arrangements at the airport (see Bellanova and Fuster, 2013).

Securitizing liquids aligns well with concerns about the unpredictable human elements of the apparatus: the security guards. As the National Coordinator for Counterterrorism explained: 'since humans are the weak link in the security process, we aim for technological innovation as the solution for airport security.'[13] By shaping and limiting the conduct of security personnel, technologies act as governing devices. Reflecting a longstanding 'rush to upgrade security by technological means' (Lyon, 2006: 407), the security director of Schiphol prefers ridding the apparatus of humans altogether, and visualizes the ideal security apparatus as completely made up of non-humans: 'I'd like to see a device that screens everyone without touching them, which leaves privacy intact and is 100% secure, without disrupting the boarding procedures of an aircraft' (G4S, 2005).

While approximating this ideal, the full body scanner initially proved too efficient: Germans called the body scanners 'nacktscanners' or 'virtual strip search', as they could reveal very detailed images of human bodies underneath clothes (*Der Spiegel*, 2009, see Figure 2). This in turn caused a 'worldwide controversy', with the European Commission and various human rights organizations voicing their concerns (Stone, 2009). Human rights became explicitly linked to the problematization of the human body through visual imageries produced by the machines; security management at Schiphol had to enrol critical audiences by turning their preferred security technology into a harmless device. Public debates on human rights and privacy in the US and Germany – not part of the 'content' of the jobs of security professionals at Schiphol – introduced new contextual actants that had to be dealt with in the stabilization of the controversy and the production of security at Schiphol.

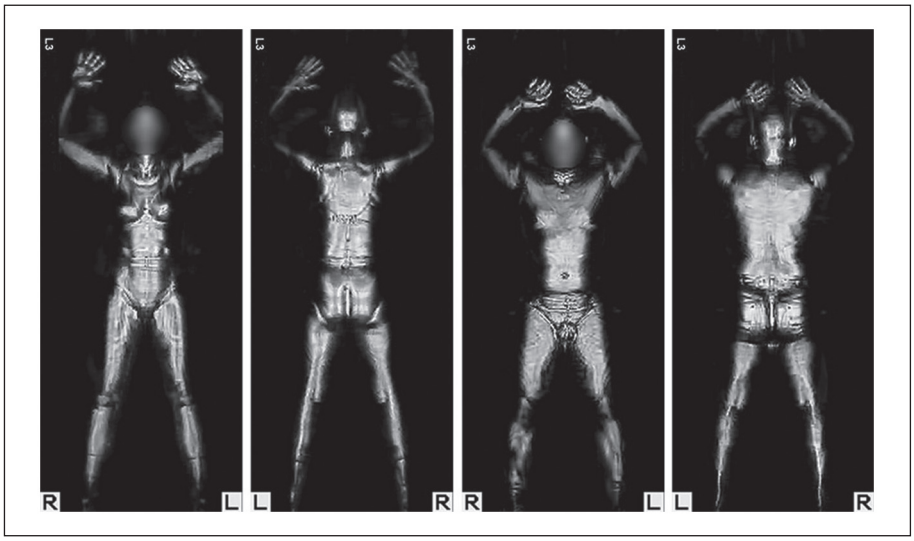

Figure 2. Image generated by L3 millimetre wave technology scanners.
Source: U.S. Department of Homeland Security, public domain.

Figure 3. Image as seen by security agent after anonymizing software has been added.
Source: Courtesy of Schiphol Airport.

As the scanner itself cannot distinguish between private and non-private parts of bodies, airport security authorities added software to the assemblage in order to render images less plastic (see Figure 3) and enlist, among others, worried passengers and German authorities behind the implementation of this technology as the new standard. In order to disassociate the scanner from the potentially sensitive issues surrounding privacy of bodies, Schiphol renamed it 'security scan' (Schiphol Group, 2012). Only after security managers addressed these controversies could the body scanner become a 'black box', redistributing agency across the security apparatus. Emerging

as a central 'actor' out of the controversy at Schiphol – the first airport to run trials with it – the scanner itself became mobile and, according to the *Daily Mail*, 'took off across the world' (Watson, 2011). In November 2011, the European Commission incorporated the security scan into European legislation as an official European security measure (Schiphol Group, 2012: 73; see Bellanova and Fuster, 2013, for elaborated discussion).

Following a period of intense controversy (2009–2011), the body scanner now forms a new actant in the security apparatus of Schiphol, and of Europe more generally. It has literally become an obligatory passage point for travellers, but only because of the many allies mobilized behind it: KPIs, the TSA, commercial interests and even, in the end, liberal rights. Airport security at Schiphol is a socio-technological apparatus that only allows for particular kinds of security solutions to be incorporated: those categories of security efforts that were impossible to translate into KPIs have been excluded, and KPIs proved a pivotal infrastructural actant resisting the translation of terrorism into a matter of human behaviour. The prevalence of the body scanner at Schiphol is the outcome of a successful securitization process for liquids and metals, and a less successful securitization of human behaviour, illustrating how during controversies 'security and insecurity can be played out through the mundane ontology of things' (Neyland, 2009: 39). By now, the number of bottles and tubes containing prohibited – and potentially dangerous – liquids that the device has detected primes as a key indicator of how secure or insecure the airport is. The body scanner, a non-human spokesperson for security at the airport, proved a more durable actant in the apparatus than 'security awareness' programmes when the latter were confronted with the resistance of KPIs (see Law, 2009: 148). Now that the airport was equipped with the latest technological security innovations, the controversy was reduced to manageable proportions. Once more, the airport came to be considered a calm and predictable entity; the security apparatus receded back to the hinterland of Schiphol. Yet by no means can it be assumed that the introduction of the body scanner definitively put an end to the controversy. Liquid requirements remain highly contested and new actants constantly challenge the security apparatus, such as, most recently, needles that managed to travel into passengers' bodies via Dutch airport catering (*ABC News*, 2012). Sometimes people, sometimes objects, such mundane entities potentially destabilize the black box of airport security, turning it again into an open controversy.

Conclusion

This article introduced actor-network theory as an alternative methodological and conceptual toolbox with which to study security as controversy. Taking security as a controversy means opening up black boxes of security governance and, rather than looking at the effects of security discourses once they are established, digging into the ontological politics of unfolding controversies. By way of conclusion, the article presents some possible implications of this approach for larger debates within security studies.

While regularly denounced as uncritical or apolitical for not taking a stance, controversy mappings are highly political acts or artifacts as, through description, they interfere politically by rendering new elements *as* matters of concern open to public scrutiny (Law and Singleton, 2000: 769–770; also see Dewey, 1927). By describing the ontological politics at work, my mapping of the controversy at Amsterdam Airport contributes to its continuing existence and its contestation (paraphrasing Barry, 2012: 331), where translations in the airport security apparatus represent a contrary movement, rendering airport security a technical matter for experts rather than a public one. This brings actor-network theory close to central concerns in critical approaches to security, where state-centric theorizing is under attack for co-performing a certain kind of world by foreclosing what security can mean. By extension, different 'turns' in security studies can equally be

considered as limiting the scope of what 'counts' on ontological premises (see Aradau et al., 2014). While restricting what matters in security studies on ontological grounds does provide analytical purchase, it also silences at least some of the complex processes of the deliberation, assembling, negotiation and translation part of the settling of security controversies (Huysmans, 2011: 377). The point of using actor-network theory to analyse security governance at Amsterdam Airport has been precisely to illustrate that when security is in the making – that is, still a controversy to be settled – it is ontologically unstable and indistinguishable from the 'context' made up of economic, technological, medical and legal considerations: the 'content' of security merges with the context, and it becomes impossible to sensibly isolate security at Schiphol Airport from, say, economic considerations, from what the *New York Times* writes about the quality of images from scanning devices, and from a Nigerian saying whether or not he did whatever he did in the name of Al-Qaeda. The end product 'security' becomes disentangled from this 'context' only owing to the efforts of actors as they try to separate out security as something concrete and distinct from 'other' considerations, in the process ontologically redistributing (in)security. Actor-network theory's critical purchase thus lies in offering us a way to study security, not in terms of stable arrangements that impress themselves upon us as powerful 'cold monsters', but rather as unsettled accounts of fragile security by entering into the controversies when security is still in the making. The other way around, and perhaps more importantly, concerns in security studies should be seen as opportunities for actor-network theory to extend its approach and address a broad range of distinct and politically urgent controversies.

Acknowledgements

I would like to thank Jan Bachmann, Didier Bigo, Anna Leander, Maximilian Mayer, Maria Stern, members of the International Collaboratory on Critical Methods in Security Studies, the editors of *Security Dialogue* and the anonymous reviewers for comments on previous versions of this article.

Funding

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Author's note

An earlier version of this article was presented at the 2010 Annual Convention of the International Studies Association and other meetings.

Notes

1. For the 'material turn' in international relations, see, most notably, the special issue of *Millennium: Journal of International Studies* (vol. 41, no. 3) on materialism; for actor-network theory in international relations more generally, see the forum in *International Political Sociology* (vol. 3, no. 7).
2. See http://mappingcontroversies.net/.
3. Exceptions to date include Bueger and Bethke (2013), Mayer (2012a) and Bourne (2012).
4. See note 1 above.
5. This does not hold for the MACOSPOL project, which creates digital snapshots folding all elements of a public controversy into single, digitally navigable events. This otherwise sophisticated mapping approach loses some of the nuance that textual methods offer for capturing the important ways in which elements matter in the unfolding of a controversy, and fails to indicate to which new patterns of governance the settling of controversies leads (see Barry, 2012: 327). Rather than following the MACOSPOL methodology, this article builds on the more qualitative ethnographic approach of actor-network theory scholars, which consists of narrating the unfolding and settling of controversies (see Loughlan et al., 2014).

6. See http://www.oxforddictionaries.com/definition/english/actant (accessed 1 November 2013).
7. To credit the human spokespersons explicitly (the textual ones will be cited throughout the article): I have interviewed key spokespersons from all elements of the airport security apparatus, including airport security managers and guards from the private security companies Group 4 Securicor, Securitas, Trigion and the International Security and Counter-Terrorism Academy; security managers of the airport itself; senior policymakers at the National Coordinator for Counterterrorism, within the Royal Constabulary and inside the Dutch government (Ministry of Justice); millimetre wave scanner experts and salespersons at the 2010 Counter Terror Expo in London; a Dutch security management journalist; and an airport security technologies researcher at the TNO (Netherlands Organization for Applied Scientific Research, the Dutch equivalent of the RAND organization).
8. Interview, Schiphol, January 2010. Unless stated otherwise, all – anonymized – quotes are from interviews conducted at Schiphol between December 2009 and July 2010.
9. Interview, The Hague, December 2009.
10. Interview, Amsterdam, January 2010.
11. Schiphol requested me not to disclose the 'content' of KPIs as they are considered strategic for airport security.
12. Interview, The Hague, July 2010.
13. Interview, The Hague, December 2009.

References

Aas KF (2012) (In)security-at-a-distance: Rescaling justice, risk and warfare in a transnational age. *Global Crime* 13(4): 1–19.

Aas KF, Gundhus HO and Lomell HM (2009) *Technologies of InSecurity: The surveillance of everyday life*. New York: Routledge-Cavendish.

ABC News (2012) Needles in sandwiches: FBI, Dutch police investigating caterer, security gaps. 17 July. Available at: http://abcnews.go.com/Blotter/needles-sandwiches-fbi-dutch-police-investigating-caterer-security/story?id=16797700 (accessed 6 April 2013).

Adey P (2009) Facing airport security: Affect, biopolitics, and the preemptive securitisation of the mobile body. *Environment and Planning D* 27(2): 274–295.

Adey P and Anderson B (2012) Anticipating emergencies: Technologies of preparedness and the matter of security. *Security Dialogue* 43(2): 99–117.

Adey P, Anderson B and Guerrero LL (2011) An ash cloud, airspace and environmental threat. *Transactions of the Institute of British Geographers* 36(3): 338–343.

Adler E and Pouliot V (2011) International practices. *International Theory* 3(1): 1–36.

Ahlers MM (2010) TSA nominee wants to move airport screening closer to 'Israeli model'. *CNN*, 23 March. Available at: http://edition.cnn.com/2010/TRAVEL/03/23/tsa.nominee.senate/index.html (accessed 27 September 2013).

Air Transport Action Group (ATAG) (2012) *Aviation: Benefits Beyond Borders*. Geneva: ATAG.

Amsterdam Airport (2007) Eenduidig toezicht Schiphol [Unequivocal oversight Schiphol]. Schiphol: Amsterdam Airport.

Amsterdam Airport (2010) *Safety & Security Pocket Guide 2010–2011*. Schiphol: Amsterdam Airport.

Amsterdam Airport (2012) Who does what in Airport Security? Available at: http://extra.aviationonline.schiphol.nl/Home/SecurityAndSchipholPass/PrivateParties.htm (accessed 1 September 2013).

Aradau C (2010) Security that matters: Critical infrastructure and objects of protection. *Security Dialogue* 41(5): 491–514.

Aradau C, Coward M, Herschinger E, et al. (2014) The matter of method: Analyzing discourses and materialities of (in)security. In: Aradau C, Huysmans J, Neal A and Voelkner N *Critical Security Methods: New Frameworks for Analysis*. London: Routledge.

Baldwin DA (1997) The concept of security. *Review of International Studies* 23(1): 5–26.

Barry A (2012) Political situations: Knowledge controversies in transnational governance. *Critical Policy Studies* 6(3): 324–336.

Barthes R (1975) An introduction to the structural analysis of narrative. *New Literary History* 6(2): 237–272.

Beck G and Kropp C (2010) Infrastructures of risk: A mapping approach towards controversies on risks. *Journal of Risk Research* 14(1): 1–16.

Bellanova R and Fuster GG (2013) Politics of disappearance: Scanners and (unobserved) bodies as mediators of security practices. *International Political Sociology* 7(2): 188–209.

Berndtsson J and Stern M (2011) 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): 408–425.

Bigo D (2000) Liaison officers in Europe: New officers in the European security field. In: Sheptycki JWE (ed.) *Issues in Transnational Policing*. London: Routledge, pp. 67–99.

Bourne M (2012) Guns don't kill people, cyborgs do: A Latourian provocation for transformatory arms control and disarmament. *Global Change, Peace & Security* 24(1): 141–163.

Brown MB (2009) *Science in Democracy: Expertise, Institutions, and Representation*. Cambridge: MIT Press.

Bueger C (2013) Actor-network theory, methodology, and international organization. *International Political Sociology* 7(3): 338–342.

Bueger C and Bethke F (2013) Actor-networking the 'failed state': An inquiry into the life of concepts. *Journal of International Relations and Development*, January 18, 2013; doi:10.1057/jird.2012.30.

Bueger C and Villumsen T (2007) Beyond the gap: Relevance, fields of practice and the securitizing consequences of (democratic peace) research. *Journal of International Relations and Development* 10(4): 417–448.

Çalişkan K and Callon M (2009) Economization, part 1: Shifting attention from the economy towards processes of economization. *Economy and Society* 38(3): 369–398.

Callon M and Latour B (1981) Unscrewing the big Leviathan: How actors macro-structure reality and how sociologists help them to do so. In: Knorr-Cetina K and Cicourel AV (eds) *Advances in Social Theory and Methodology: Towards an Integration of Micro- and Macro-sociologies*. London: Routledge, pp. 277–303.

Coole D and Frost S (2010) *New Materialisms: Ontology, Agency, and Politics*. Durham, NC: Duke University Press.

Dahlkamp J, Evers M, Rosenbach M and Stark H (2010) Scanner mania vs. profiling: Are traditional security methods the best path to air safety? *Der Spiegel*, 4 January. Available at: http://www.spiegel.de/international/europe/scanner-mania-vs-profiling-are-traditional-security-methods-the-best-path-to-air-safety-a-669968.html (accessed 1 November 2013).

De Jong B (2012) *The Airport Assembled: Rethinking Planning and Policy Making of Amsterdam Airport Schiphol by Using the Actor-Network Theory*. Utrecht: Utrecht University.

De Vries G (2007) What is political in sub-politics? How Aristotle might help STS. *Social Studies of Science* 37(5): 781–809.

Der Spiegel (2009) New airline security measures are 'blind overreaction'. 29 December. Available at: http://www.spiegel.de/international/world/the-world-from-berlin-new-airline-security-measures-are-blind-overreaction-a-669418.html (accessed 1 November 2013).

Dewey J (1927) *The Public and Its Problems*. New York: Henry Holt and Company.

Engelhardt HT, Jr and Caplan AL (1989) *Scientific Controversies: Case Studies in the Resolution and Closure of Disputes in Science and Technology*. Cambridge: Cambridge University Press.

Feldman G (2011) If ethnography is more than participant-observation, then relations are more than connections: The case for nonlocal ethnography in a world of apparatuses. *Anthropological Theory* 11(4): 375–395.

Foucault M (2007) *Security, Territory, Population: Lectures at the Collège de France, 1977–1978*. New York: Picador.

G4S (2005) Aviation security: Freedom or protection? *G4S International Magazine* (September): 29–31.

Hale A (2001) Regulating airport safety: The case of Schiphol. *Safety Science* 37(2–3): 127–149.

Huysmans J (2011) What's in an act? On security speech acts and little security nothings. *Security Dialogue* 42(4–5): 371–383.

Jones R (2009) Checkpoint security: Gateways, airports and the architecture of security. In: Aas KF, Gundhus HO and Lomell HM (eds) *Technologies of InSecurity: The Surveillance of Everyday Life*. Milton Park: Routledge-Cavendish, pp. 81–101.

Kendall G (2004) Global networks, international networks, actor networks. In: Larner W and Walters W (eds) *Global Governmentality: Governing International Spaces*. London: Routledge, pp. 59–75.

Klauser FR (2009) Interacting forms of expertise in security governance: The example of CCTV surveillance at Geneva International Airport. *The British Journal of Sociology* 60(2): 279–297.

Klauser FR, Ruegg J and November V (2008) Airport surveillance between public and private interests. In: Salter MB (ed.) *Politics at the Airport*. Minneapolis, MN: University of Minnesota Press, pp. 105–126.

Latour B (1987) *Science in Action: How To Follow Scientists and Engineers Through Society*. Cambridge: Harvard University Press.

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

Law J (2009) Actor network theory and material semiotics. In: Turner BS (ed.) *The New Blackwell Companion to Social Theory*. Oxford: Blackwell, pp. 141–158.

Law J and Callon M (1988) Engineering and sociology in a military aircraft project: A network analysis of technological change. *Social Problems* 35(3): 284–297.

Law J and Singleton V (2000) Performing technology's stories: On social constructivism, performance, and performativity. *Technology and Culture* 41(4): 765–775.

Lippert R and O'Connor D (2003) Security assemblages: Airport security, flexible work, and liberal governance. *Alternatives: Global, Local, Political* 28(3): 331–358.

Lipton E and Shane S (2009) Questions on why suspect wasn't stopped. *New York Times*, 27 December.

Loughlan VE, Olsson C and Schouten P (2014) Mapping security practices as critical methodology: Exploring the potential of Bourdieu and Latour. In: Aradau C, Huysmans J, Neal A and Voelkner N *Critical Security Methods: New Frameworks for Analysis*. London: Routledge.

Lyon D (2006) Airport screening, surveillance, and social sorting: Canadian responses to 9/11 in context. *Canadian Journal of Criminology and Criminal Justice* 48(3): 397–411.

MacKenzie DA (2006) *An Engine, Not a Camera: How Financial Models Shape Market*. Cambridge: MIT Press.

McSweeney B (1999) *Security, Identity, and Interests: A Sociology of International Relations*. Cambridge: Cambridge University Press.

Marcus GE and Saka E (2006) Assemblage. *Theory, Culture & Society* 23(2–3): 101–106.

Marres N (2007) The issues deserve more credit: Pragmatist contributions to the study of public involvement in controversy. *Social Studies of Science* 37(5): 759–780.

Marres N and Lezaun J (2011) Materials and devices of the public: An introduction. *Economy and Society* 40(1): 489–509.

Mayer M (2012a) Chaotic climate change and security. *International Political Sociology* 6(2): 165–185.

Mayer M (2012b) *How IR Might Overcome Its "Lightness": Technological Innovations, Creative Destruction, and Explorative Realism*. Bonn: University of Bonn.

Melman Y (2010) Israeli firm blasted for letting would-be plane bomber slip through. *Haaretz*, 10 January.

Mitchell T (2009) Carbon democracy. *Economy and Society* 38(3): 399–432.

Mol A (1998) Ontological politics: A word and some questions. *Sociological Review* 46(S): 74–89.

National Coordinator for Counterterrorism (NCC) (2006) Gezamenlijk cameranetwerk Schiphol van bedrijfsleven en overheid [Collective camera network for business and government at Schiphol]. Archived press communiqué.

National Coordinator for Counterterrorism (NCC) (2009) NCTb helping companies and organisations strengthen security. Available at: https://english.nctv.nl/currenttopics/press_releases/2009/press_release_091008.aspx?cp=92&cs=66055 (accessed 1 October 2013).

Neumann IB (2007) 'A speech that the entire ministry may stand for,' or: Why diplomats never produce anything new. *International Political Sociology* 1(2): 183–200.

New York Times (2009) Technology That Might Have Helped. 27 December. Available at: http://www.nytimes.com/interactive/2009/12/27/us/terror-graphic.html?_r=0.

Neyland D (2009) Mundane terror and the threat of everyday objects. In: Aas KF, Gundhus HO and Lomell HM (eds) *Technologies of InSecurity: The Surveillance of Everyday Life*. Milton Park: Routledge-Cavendish, 21–41.

NRC Handelsblad (2009a) NCTb: Terrorismeverdachte volgens procedures gecontroleerd [NCC: Terrorism suspect checked according to procedures]. 26 December. Available at: http://vorige.nrc.nl/binnenland/article2445969.ece.

NRC Handelsblad (2009b) Unused body scan could have revealed explosive powder. 28 December. Available at: http://vorige.nrc.nl/article2446632.ece.

Pyyhtinen O and Tamminen S (2011) We have never been only human: Foucault and Latour on the question of the anthropos. *Anthropological Theory* 11(2): 135–152.

Reuters (2009) Timeline of attempt to blow up U.S. airliner. 26 December. Available at: http://www.reuters.com/article/2009/12/26/us-security-airline-timeline-idUSTRE5BP20920091226 (accessed 10 October 2013).

Salter MB (2008a) Imagining numbers: Risk, quantification, and aviation security. *Security Dialogue* 39(2–3): 243–266.

Salter MB (2008b) *Politics at the Airport*. Minneapolis, MN: University of Minnesota Press.

Salter MB (2008c) Securitization and desecuritization: A dramaturgical analysis of the Canadian Air Transport Security Authority. *Journal of International Relations and Development* 11(4): 321–349.

Salter MB and Mutlu CE (2012) *Research Methods in Critical Security Studies: An Introduction*. London: Routledge.

Schiphol Group (2011) *Annual Report 2010*. Schiphol: Schiphol Group.

Schiphol Group (2012) *Annual Report 2011*. Schiphol: Schiphol Group.

Schouten P (2013) The materiality of state failure: Social contract theory, infrastructure and governmental power in Congo. *Millennium: Journal of International Studies* 41(3): 553–574.

Smith S (1999) The increasing insecurity of security studies: Conceptualizing security in the last twenty years. *Contemporary Security Policy* 20(3): 72–101.

Stone M (2009) Full body scanners for airport security cause worldwide controversy. *The Examiner*, 30 December.

Valverde M (2011) Questions of security: A framework for research. *Theoretical Criminology* 15(1): 3–22.

Van den Dongen J and Olmer B (2009) Zware kritiek op knullige controle: Ex-medewerkster met zwijgplicht doet boekje open [Heavy criticism on clumsy monitoring: Ex-employee with oath of secrecy speaks out]. *De Telegraaf*, 28 December.

Van der Kloor R (2010) PvdA eist hoorzitting beveiliging Schiphol [Labor Party demands hearing on Schiphol security]. *Elsevier*, 4 January.

Venturini T (2010) Diving in magma: How to explore controversies with actor-network theory. *Public Understanding of Science* 19(3): 258–273.

Voelkner N (2011) Managing pathogenic circulation: Human security and the migrant health assemblage in Thailand. *Security Dialogue* 42(3): 239–259.

Vuori JA (2008) Illocutionary logic and strands of securitization: Applying the theory of securitization to the study of non-democratic political orders. *European Journal of International Relations* 14(1): 65–99.

Watson L (2011) Airport scanners that 'strip' passengers naked are banned over fears they cause cancer. *Daily Mail*, 17 November. Available at: http://www.dailymail.co.uk/news/article-2062608/Naked-airport-scanners-banned-fears-cause-cancer.html.

Peer Schouten is a PhD candidate at the School of Global Studies/University of Gothenburg and Editor-in-Chief of *Theory Talks*.