Between Public and Private: The Co-production of Infrastructural Security

Nolte, A.; Westermeier, C.

DOI
10.1080/02589346.2020.1712831
Publication date
2020
Document Version
Final published version
Published in
Politikon

POLITIKON
2020, VOL. 47, NO. 1, 62–80
https://doi.org/10.1080/02589346.2020.1712831

Routledge
Taylor & Francis Group

Between Public and Private: The Co-production of Infrastructural Security

Amina Nolte[a] and Carola Westermeier[b]

[a]Department of Sociology, Justus-Liebig-University of Giessen, Giessen, Germany; [b]Department of Political Science, University of Amsterdam, Amsterdam, The Netherlands

ABSTRACT
The paper proposes to use the concept of co-production to account for the mutual co-production of private as well as public security actors and critical infrastructure. Through an exploration in the field of urban security provision, we aim to contribute to critical security studies by turning to the entanglements of public and private security actors in the process of securitising infrastructure. As the construction and provision of infrastructural security depends neither solely on public nor private actors but on their interaction, we propose the concept of co-production to account for these dynamics. Based on a focused ethnography, the paper mobilises material collected during a security conference in Israel, in which the close connections between private and public security actors were forged and where infrastructure was at the heart of the security concerns.

Introduction

> So, as we come out of the army, we're in life and death situations in the army, and we come out to the world, and we all believe that we could be the next Mark Zuckerberg, we are going into technology and come up with all these cool new start-ups. (Interview, Safe and Smart City Conference, November 19th, 2018)

Amidst the *Safe and Smart City* Conference that took place in Jerusalem in November 2018, a former general in the Israeli Defense Forces (IDF) spoke about his experiences in the army and the booming private security industry in Israel. Based on first-hand qualitative material that we collected as participants of the conference and interviews we conducted, we aim to contribute to current debates in Critical Security Studies (CSS). In particular, we discuss the interaction between public and private actors within the field of security by highlighting the co-production of security concerns and expertise. Set up around the safety and security of urban environments in the twenty-first century, the *Safe and Smart City Conference* gathered European and Israeli policy leaders, security companies and representatives of public institutions such as local municipalities for an exchange of best practices in the Waldorf Astoria Hotel, Jerusalem.

Organised and financed by the European Network Elnet the aim was establishing and deepening exchanges on policy issues between Israeli and European policy makers, innovators and business leaders, the gathering in Jerusalem addressed security issues and challenges in and around cities. The conference programme comprised topics related to quality of life, the improvement of public services, the safety of sensitive infrastructures, and the vulnerability of intelligent systems under the overarching theme *Better life, safer*

CONTACT Amina Nolte amina.nolte@gmx.net

world and shared values.[1] Those topics, approaches and the way they were discussed reveal the intricacies of contemporary security politics, especially with regard to the mutual constitution of shared assumptions and networks of expertise.

The concern regarding so-called critical infrastructure and the discussion of possible solutions to make infrastructure safer is shared by public and private security actors, not only in Israel. Infrastructures, the socio-material substrate of urban life, are at the heart of contemporary security considerations all over the world since their failure has proven fatal in case of natural disasters, terror attacks and other forms of breakdown (Lakoff and Collier 2010). The issue of their security combines many topics that are increasingly of concern to policy makers, urban planners, public authorities and private actors. One crucial aspect in the provision of the security of infrastructure is the maintenance of forms of mobility, allowing for people, goods, resources and technologies to circulate without interruption while at the same time blocking 'dangerous' elements from the circulation. Seen from the perspective of enabling circulation as sustaining everyday life, infrastructure protection has therefore gained much attention as one crucial aspect of urban security programmes.

The focus of this paper thus lies on the securitisation of infrastructure and the productive processes around the production of its criticality. We are interested in how infrastructures are rendered critical by ways of securitisation and how this process is (co-)productive of actors and the blurring of presumably clearly defined fields of public and private. We aim to contribute to literature on public-private security interactions by proposing the notion of *co-production* as a conceptual frame to analyse the dynamics between public and private security actors in the process of securitising infrastructure. We also follow the distinction and denomination of *public* and *private* that has been proposed by the literature that explores these intersections (Abrahamsen and Williams 2009). The public-private distinction seems more suitable than descriptions as 'commercial', 'economic' or 'state' actors as these characteristics do not apply for the diversity of actors that are at play.

Following the claim that security is not an objective reality but rather 'what actors make of it' (Buzan and Wæver 2003, 48), this contribution accounts for the deeply intersubjective situatedness of security concerns and problems. By scrutinising the *Safe and Smart City Conference* in Jerusalem we hence explore a concrete and situated process in which security concerns are produced around the concern for urban security. Further, and in line with the constructivist approach towards security, we understand the expertise and experts that produce security concerns as equally 'produced' through these interactions. We underscore the relational understanding of securitisation processes (Langenohl 2019) by bringing insights from the field of Science and Technology Studies (Jasanoff 2004) into the (critical) study of security (see also de Goede 2018).

The paper proposes the concept of *co-production* to better understand why and how infrastructures are securitised and how this in turn produces the fields of private and public security actors. We approach the construction and provision of security not merely by looking at the cooperation between ostensibly separate public and private actors, but emphasise the mutual co-production across those spheres. We contend that the public and the private are not two realms that can be analysed apart from each other because infrastructure provision and infrastructure protection is not exclusively a public and/or private concern either. Rather, the invention, construction, maintenance

and protection of infrastructures as critical is bound to the specific expertise of *both* public and private spheres. Moreover, public and private actors 'produce' critical infrastructure, but they are also a product of this process. They are constituted as public or private as they are addressed in these regards. As such, the process of rendering infrastructure critical is a twofold and thus productive process: by constructing infrastructure as endangered, threatened and thus potentially critical, the need for the expertise of these differing actors is produced, which in turn produces the need for their respective knowledge to protect the defined critical infrastructure.

The structure of the paper as follows: first we contextualise our paper in the existing debates in CSS and explain the gap we seek to fill by adding a co-production perspective. We then give a brief introduction into the fluidity between public and private actors and their cooperation in Israel in order to introduce the conference setting in which the research mostly took place, followed by an explanation of our methodological approach and our understanding of the research as 'focused ethnography'. In the empirical part, we discuss the concept of co-production and relate it to the field of public and private actors and their mutual co-production through and of critical infrastructure. We first discuss how security experts construct themselves in the process of securitising infrastructure. In a second step, we show how the production of (digital) critical infrastructure always entails the production of public and private actors. In conclusion, we discuss our findings and some questions that arise from the presented research.

The public-private divide and its limits

Commercialisation, privatisation and financialisation of security

A broad range of contributions to Critical Security Studies have analysed the complex ways in which security efforts depend on private actors, or how vital tasks within national security have been handed to private companies (Avant 2005; Krahmann 2008; Neocleous 2007; Leander 2005, 2010, Joachim and Schneiker 2018). The study of private security actors thereby encompass a wide array of topics, such as the contribution of private security actors to the construction of (in)security and disastrous futures (Hoijtink 2014), the fluid exchange of personnel between the military and private companies (Grassiani 2018), or the enforcement of neoliberal governmentality by private security contractors (Leander and van Munster 2007). The financialisation of security has been described for the field of financial security as banks act as security actors (Amicelle 2011). Surveillance studies have also emphasised the close entanglements of state and private surveillance. David Lyon (2009) has described how state surveillance depends on market technology and Ben Hayes highlights new alliances between the state-surveillance and the military-industrial complex (Hayes 2014). The empirical examples are thus diverse and recent developments even seem to indicate an intensification of these developments.

For Rita Abrahamsen and Anna Leander (2016), the expansion of private security has a number of reasons: Already with the advent of post-Fordism, partnerships between public and private actors and 'outsourcing' became a central feature of economic life. In addition, innovations in (military) technologies developed by private companies made them indispensable for these purposes. More generally, the dominance of neoliberal forms of government led the market to become a core focus of the governance of security. Private

security actors are widely established and considered normal in the field of security. And they have increased in quantity. Recently, Elke Krahmann (2018) has pointed out that there are now nearly as many private security guards employed as public police forces in Europe, contributing to the perception that the EU and other political entities have failed as collective security communities. Similar observations have also been made for a range of other countries on all continents (Abrahamsen and Williams 2009).

Regarding the sheer quantity of private security efforts, it is surprising that, analytically, they are still perceived differently from 'classical', meaning public security actors, such as the military or the police. We can find numerous accounts in which a mostly implicit assumption seems to be that security is better placed within the domain of the state, or at least that the state should hold the prerogative to decide how security is managed (Volinz 2018). The provision of security is thus still portrayed as a primary task of the state as its original 'owner'.

The assumption that tasks of security have 'moved' from the state to private actors is also reflected in the concepts that are used to describe the interplay between public and private actors. While a number of scholars have employed the concept of *assemblage* to describe the heterogeneous parts and actors that come together in the provision of security (Abrahamsen and Williams 2009; de Goede 2012), others have used more processual concepts to describe security practices. Anna Leander (2010) has argued that the term *privatisation* has limitations, preferring the term *commercialisation* (or *commodification*, see Neocleous 2007) as this highlights how these processes define security and how it is practiced within public and private institutions. However, concepts such as privatisation and commercialisation also rely on a stark division between the public and the private sphere and may even evoke such divisions.

Strict divisions of public and private actors within the field of security have been subject to criticism. Most outspokenly, Mark Neocleous is advocating a very different stance in his fundamental critique of security. He argues that privatisation does not adequately describe the changes that occur within the provision of security. He finds these assessments to reinforce the division of state and capital that is based on liberal understandings of the state. He instead proposed a Marxist understanding that understands these forces to be unified in their 'obsession with security' (2007, 349). Acknowledging the role of security as 'the basis for both a sustained capital accumulation and a constant political policing of civil society' would allow to focus on the ongoing 'commodification of security' (Neocleous 2007, 349).

We agree with Neocleous that the notion of privatisation is misleading inasmuch as it takes the state as a starting point of analysis and assumes that its responsibilities are increasingly taken over by private actors. However, this does not necessarily lead us to agree with Neocleous's Marxist understanding of state and capital as one unity and his conclusion to give up on the distinction between private and public altogether. Instead, we argue that we need to refine our understanding of the commonalities and contradictions of these entanglements between state and private actors. Hence, we explore the space between Neocleous's understanding of public and private efforts to be mutually following the 'fetish of security' on the one hand and studies that assume a fundamental distinction between the two spheres and their underlying aims on the other. Within the latter, it is often insinuated that security practices should lie with (or return to) the state because this would entail the provision of security as a public good and less as a commodity.

Discussing the securitisation of infrastructures shows the broad space between these differing assessments, urging us to rethink them altogether with regard to digitalised infrastructures.

In proposing the concept of co-production for the study of public-private security interactions, we follow Abrahamsen and Williams (2009) understanding of the heterogeneous 'complex security networks that knit together public and private, global and local actors'. They argue that it is misleading to situate

> security actors in a zero-sum game of opposition to public power. While there is little doubt that private security may in certain settings be an indication of state weakness or pose a threat to the state, such interpretations overlook the manner in which the empowerment of private actors is directly linked to transformations inside the state and often takes place with the active endorsement and encouragement of state authorities. (6)

In line with their argument, Shir Hever has also argued that in the Israeli case,

> state officials promote the privatisation of security not just out of weakness, but for more complex reasons. There is a porous border between the state elites and the private sector elites, and those elites dealing with security can be considered as an elite group. (2018, 14)

In our contribution we consider the interplay of public and private actors in the securitisation of infrastructure within the Israeli context to be most instructive for the dynamics of co-production.

Critical infrastructure at the interstices of public and private security actors

The concept of critical infrastructure has received increased attention in CSS since the unfolding scholarly debates after 9/11 and the associated question of the vulnerability of infrastructure to breakdowns and terror. James Peter Burgess (2007) analyses European Strategies to protect critical infrastructure in response to 9/11 as well as the terror attacks in Madrid and London. He sees the criticality of infrastructure to be determined by its highly symbolic cultural and value. Collier and Lakoff (2010) highlight how the vulnerability of critical infrastructure has become an object of knowledge for security experts in the United States. They locate the US plans for the protection of critical infrastructure within a strategy that they call the 'political technology of preparedness' (2010, 244). Claudia Aradau (2010) gives space to the role of materiality in the securitisation of infrastructure. Her contribution is very helpful for our argument in two ways: First, she argues that labelling infrastructures as 'critical' for the purposes of protecting them against terrorist attacks is a securitising move (501). Second, by highlighting how critical infrastructure materialises as a specific socio-material constellation that is produced through discourses and practices, Aradau implies, although with different intention, the productive force of infrastructure that materialises as critical.

In a more recent discussion on what makes critical infrastructure critical, Andreas Folkers (2018) notes that the provision of infrastructure has increasingly become a task that is shared between the state and private actors. However, since the 1990s the provision of infrastructure is not in the hands of a centralised actor or institution anymore but has diffused into a plurality of providers and operators. Further, Folker's contribution is important to our argument as it highlights that criticality is not an objective term but that every definition of criticality implies the attribution of value to specific infrastructures (2018,

124). Picking up on this argument, we will show that the question of what infrastructure is deemed critical is part of a complex process of political and social negotiations. Critical infrastructure is produced politically – and at the same time highly productive of political moments and modes of differentialisation. This means that – once rendered critical – infrastructure can turn into a site of producing difference by providing the means and justification for the channelling, sorting and separating of wanted and non-wanted mobilities.

Public–private fluidity in Israel

This paper derives its empirical material from a conference setting in Israel. Thus, it is worth to look at the Israeli security scene to understand the close ties that exist between the military and the private sector as a driving force of security policies, technologies and the international interest in learning from best practices in Israel (Machold 2016).

Most Israeli men and women[2] are conscripted to the Israeli Defense Forces (IDF) after finishing school. After completion of the mandatory service, Israelis stay closely associated with their former unit, while male soldiers might be called in for reserve duty once a year (Halper 2015, 39). For many Israelis, an employment in the private security sector is very common either after finishing the mandatory army service or after retiring from a successful military career (Hever 2018, 14). The start-up sector in Israel booms with new companies offering their service in the field of security (Hever 2018, 155). Thus, coming from serving in the military for at least two or three years, oftentimes more, seeking employment or setting up companies in the vibrant security industry in Israel is a common step (mostly for men).

Trained by a public institution such as the IDF, those who transfer into the private security sector experience feelings of ambivalence throughout this process. As Grassiani has put it in her in-depth study of the self-perception of Israeli security experts, they are keen to emphasise their military past while at the same time differentiating themselves from the military by stressing their unique skills as security professionals (Grassiani 2018, 84). However, these security professionals claim a great amount of legitimacy from their previous work and experience as soldiers, officers and generals in the IDF (Grassiani 2018, 84). This is reflected in the global interest in Israeli security expertise (Graham and Baker 2016, 50; Machold 2016; Stockmarr 2016, 61). As the statement from the CEO of a security company at the beginning of this paper indicates, former soldiers, working in the field of private security derive experience, dedication and legitimacy from their experience and the knowledge gained during their time as soldiers. They feel that they 'look at stuff in a very unique perspective' and have something to bring 'to the world economy and world in general'.[3]

Moreover, the existing close links between the IDF and security professionals in the private sectors do not only work towards one side: the Israeli military also actively drives the development of security expertise and technology (Halper 2015, 37). Private companies therefore research, develop and produce according to the (anticipated) demands of the military and even with the mandate of the IDF to do so (Halper 2015, 258). Thus, the limits and borders between Israeli army as a public institution and the countless private security firms are blurred in many ways. While many forms of cooperation of actors and interests exist in Israel itself, these developments are more recently 'being accompanied by policy interventions, including those of a specifically *transnational* character' (Machold 2016, 4).

This development can be well observed with regard to the countless programmes that Israeli companies offer to a global audience within the field of urban security. Here, the idea of learning from Israel as a form of transnational policy learning has become increasingly salient as a strategy of contemporary urban security governance (Halper 2015, 267; Machold 2016, 13). Many programmes offer security solutions for urban environments, tailored to the needs of (aspiring) global cities in the Global West and South.

Part of this is the continuous marketing and promotion of the programmes and expertise to a global market. While being present at global security fairs, many Israeli companies have also developed other formats to market their expertise in homeland security into a commodity that can be adjusted and tailored to the needs of other cities (Halper 2015, 269). In the following, we present an example of a conference which brings together European and Israeli policy makers, Israeli security companies and start-ups around the question of 'Safe and Smart Cities'.

Blurred lines at the smart and safe city conference

> Safe & Smart City is the Premier Europe-Israel event gathering industry leaders, innovators and Policy Makers for crossover conversation, inspiration and business opportunities.[4]

The third edition of the *Conference Safe and Smart City* is a scene where the blurring of the boundaries between public and private actors and institutions in the field of global security cooperation can be exemplarily observed. Based on previous exchanges, the atmosphere of the conference ranged between a conference, a security fair and an exchange of best practices between urban security experts and innovators. At times, the meeting reminded us of a gathering among old friends and led us to the understanding that many of the conference participants had known each other from before and other settings – or at least from the previous conferences that were held in Nice and Tel Aviv. The conference, as it seemed, was not intended to kick off a cooperation between the different fields of security industry and policy makers. Rather, it seemed as if it was celebrating and intensifying an already ongoing and vibrant cooperation to which new ideas, innovations and technologies were constantly added.

While there was a wide range of policy makers, military officials and security businesses present from the Israeli side, most of the international guests were policy makers, municipal representatives and MPs from France. Already at the opening of the meeting, it was mentioned that the French participants were eager to learn from Israeli security expertise and best practices. Stressing the experience with terrorism in urban centres in France such as in Paris (November 2015) and Nice (July 2016), many of the opening statements of the French participants suggested that Israeli and French security officials and companies were closely cooperating, for example 'to make Nice more safe'. Nir Barkat, then mayor of Jerusalem, introduced the city as one of the safest cities in the world, suggesting a 'civil' approach to urban security in which cities should not allow themselves to be turned into warzones through terror. Emphasising the close cooperation between the Jerusalem municipality, Israeli security companies and the city of Paris after the major attacks in 2016, Barkat was eager to portray Israel's – and here especially Jerusalem's – expertise in the management and containment of terrorist attacks.

Held at the prestigious Waldorf Astoria Hotel next to the Old City Walls of Jerusalem (and close to the Green Line that is still the internationally recognised border between a Jewish Israeli Jerusalem and an Arab-Palestinian Jerusalem), the conference started with an impressive Gala Dinner in the evening before the conference day. Providing for a five-star menu and free drinks for approximately 100 guests, we felt we were being allowed into a very intimidate circle of friends in which our existence was not questioned. Being openly asked about our interest and role in the conference, people would nod approvingly and suggest that universities should be much more involved in the issue of researching and providing security. This leads us to a reflection on our methodological approach to the conference setting, our participation in the conference as well as on our own position as researchers in the context of the conference.

Focused ethnography at a security conference

As officially registered participants of the conference, we employed the method of a 'focused ethnography' (Knoblauch 2005) to collect our empirical material from which we derive our analysis. Following the 'focused ethnography' approach helped us to make sense of the conference as a field site that was not durable, stable and did not allow for extensive data collection. Conferences and gathering of professionals, as in their nature, are events that allow for a short and intensive immersion of the researcher into the field. They offer the perfect setting for a focused ethnography since, according to Knoblauch, 'focused ethnographies are short-ranged and not continual'. Fields visits are bounded and short-term engagements of the researcher with his/her field and 'they may even exist only in certain intervals, such as events' (Knoblauch 2005).

Thus, for this paper, we take the conference in Jerusalem as a starting point for an explorative investigation of the contemporary security 'scene' in Israel and its attempts to translocalise its expertise and knowledge. Focusing on the exchange of knowledge, expertise and new technologies, our focused ethnography is characterised by a turn to 'structures and patterns of interaction' (Knoblauch 2005). The intensity of data collection during these two days and the material at hand from the conference allows for an 'empirical orientation towards the details of social practice' (Knoblauch 2005). Attending a conference of security practitioners and professionals, we entered a field of expertise that allowed for our presence and participation but nevertheless revealed the difference between the actor's interests in cooperation and our interest in the analysis of these forms of interaction. However, being familiar with the field of security, its terms and procedures, the focused ethnography, as opposed to other forms of observation, allowed for an intense immersion and participation in the activities, conversations and discussions of the conference during which we were approached as natural partners and colleagues rather than as strangers to the field.

Our interest in the production of critical infrastructure and the expertise around it allows for an analytical focus during the conference. We were able to follow the unfolding dynamics between private and public actors at the event and observe the ways of their interaction. Rather than assuming actors with fixed roles and interests at the conference and 'instead of imposing a pre-established grid of analysis upon these', we follow 'the actors in order to identify the manner in which these define and associate the different elements by which they build and explain their world' (Callon 1984, 201). This allows for

an open-ended investigation into the processes of cooperation and co-constitution in the field of security practice, attending to 'the actors and explain how they define their respective identities, their mutual margins of manoeuvre and the range of choices which are open to them' (201). As such, the conference enabled and created specific constellations and roles which bridge forms of social cooperation and forms of security cooperation. Herein we found ourselves within exactly those social interactions that were intended to initiate the very cooperations and processes of co-production that our research was interested in researching.

During the conference, we attended panels that raised different topics and featured different fields of expertise and we were able to 'book' appointments with specific experts in allocated time slots, thus enabling a way to deepen the conversation and explain our interest openly. In this way, we interacted with some of the conference participants in a very formal setting in which we gathered first-hand insights and materials from security practitioners. We conducted around ten 30–45 min individual interviews in which we sat with the security experts and followed up on what they had mentioned on stage, recording the interview upon approval of the interlocutor.

Our open questions covered the personal background of the expert, his (in this case only his) career path and assessment of the Israeli security scene. Further, we asked more specific questions on the role of infrastructure for security considerations, on solutions offered from the respective company and the technologies at hand in order to provide these solutions. All interlocutors were very open to our interest and willingly answered our questions. Thus, we were able to enter a positionality at the conference that allowed us to articulate our research interests, in accordance with the conference's official aim to serve as a hub for security related knowledge.

The co-production of critical infrastructure and expertise

Securitising infrastructure(s)

Panels and expert talks at the conference circled around the notion of critical infrastructure, its assessment and the presentation of technologies invented to protect infrastructures. The promotion of other forms of 'securitising infrastructures', namely technologies developed in order to secure infrastructural arrangements, included drones, sensors and smart applications. Asked what makes an infrastructure critical in the first place, Tomer Avishai (name changed), an Israeli security official we interviewed, was quick to explain that every infrastructure has the potential to be or become critical. Mentioning that infrastructure can face two forms of threats, he explained that *internal threats* stem from the infrastructure itself, while *external threats* are something that is done to the infrastructure from outside.[5]

His distinction between the internal and external threats faced by infrastructure points to the complexity of infrastructures as socio-material arrangements that are neither purely technologically driven nor solely based on or managed by human control. Any attempt trying to grasp what infrastructure is has to come to terms with the fact that infrastructures evade a clearly bounded definition. This said, any definition may start with understanding infrastructures as 'extended material assemblages that generate effects and structure social relations, either engineered (i.e. planned and purposefully crafted) or non-

engineered (i.e. unplanned and emergent) activities' (Harvey, Bruun Jensen, and Morita 2017, 5). As such, they 'are doubly relational due to their simultaneous internal multiplicity and their connective capacities *outwards*' (5).

However, constructing infrastructures as vulnerable in their nearly perfect functionality, entails a specific bias of the imagination of infrastructures itself. Historically and conceptually, infrastructure entail a highly modernist notion in which the working of infrastructure is strongly associated with a state's and society's self-narration as inherently functional and modern (Nolte and Ozdemir 2018, 8). The construction of infrastructure as vulnerable has thus tied to a modernist bias in which the threat to a specific infrastructure is constructed as threatening the state and society as such.

This modernist imagination of infrastructure is thus prone to the threats that Tomer Avishai had mentioned to us during the conference. As the material enablers of forms of circulation, such as information, resources and goods, but also the mobility of people and things, infrastructure is imagined and constructed as functioning smoothly to enable modern everyday life. As a result of this understanding of infrastructure as vital systems that keep society going, the maintenance and security of these systems has taken centre stage in the contemporary security field. Since the 'growing dependence of citizens on centrally provided infrastructure services corresponds to the growing capacities of states and large corporations to provide vital services to the networked population' (Folkers 2017, 858), the potential vulnerability of infrastructure has become a field in which concerns and calls to action for the security of infrastructure proliferate.

The complexity of infrastructure and its potential to become constructed as critical is thus twofold: On the one hand, their multiplicity relates to what the Tomer Avishai has labelled 'internal threats'. This means that the material form of the infrastructure, its technical setup or some of the flows it provides may become dangerous to the infrastructure itself. On the other hand, an infrastructure's 'connective capacities outwards' relate to what he mentioned about the external threats to infrastructure. This implies one infrastructure's capacity to affect the working of other infrastructures and keep them from functioning or stop them from working. This again would result in cascading effects of failing infrastructures in which entire cities or states could face infrastructural breakdowns, potentially resulting in chaos, the spread of diseases, economic crisis and political turmoil. With catastrophic scenarios of entire cities or states collapsing due to infrastructural breakdowns, 'infrastructures- and in particular connected nodes- are now seen as fragile and vulnerable to threats coming from ever-expanding list (sic!) of outside threats- terrorists, hackers, eco-saboteurs, bored kids and revolutionaries' (Wakefield 2018, 4).

Not every infrastructure is in itself critical since 'criticality is not an ontological assertion. Infrastructures cannot be critical as such, but only in relation to something that is depending on them' (Engels 2018, 15). Critical infrastructure, thus, is the outcome of a process in which some infrastructures get to be produced as critical vis-à-vis specific assessments of its vulnerability – and its assigned value for a nation's or population's survival. When Tomer Avishai mentioned to us during the conference that every infrastructure has the potential to become critical, he himself pointed to the process of securitising infrastructure. This implies, according to CSS, that an infrastructure's criticality evolves as the outcome of security discourses and practices. Conferences, such as the one focused on in this paper, form part of these broader discourses. In this process of production, only some infrastructures materialise as 'infrastructures to be protected at the national level' while

at the same time 'other materialities are relegated outside the purview of government' (Aradau 2010, 508).

The production of critical infrastructure is thus a 'securitizing move', these infrastructures are perceived as threatened and thus in need of special protection. However, not only does critical infrastructure evolve as the product of expert discourses, forms and problematisations. Infrastructure, once produced as critical, is 'productive' as well: it produces its own experts, threats and may bring about effects that are not intended in its production but may still result from it.

Co-production – conceptualising dynamics and interconnections

We take co-production as a concept and approach from Science and Technology Studies (STS) in which it has proven helpful to study the ways in which technology and society are mutually constitutive and do not precede or exclude one another. As one of the most prominent advocates of the co-production approach, Sheila Jasanoff suggests that the idiom of

> co-production offers new ways of thinking about power, highlighting the often invisible role of knowledges, expertise, technical practices and material objects in shaping, sustaining, subverting or transforming relations of authority. To sociologists and social theorists, the co-production framework presents more varied and dynamic ways of conceptualizing social structures and categories, stressing the interconnections between the macro and the micro, between emergence and stabilization, and between knowledge and practice. (Jasanoff 2004, 4)

The relational aspect of political and social processes and the empirical orientation of the co-production idiom as part of STS (Harbers 2005, 262) makes co-production a fruitful concept to frame the empirical findings for this paper. It is helpful to analytically frame how the actors at the conference did not only refer to one another, their interests or any technological solutions, but to account for the ways in which they mutually *produced each other* in their positionality within the public and the private sphere. Within their interactions, they also co-produce the very socio-technical security problems that they suggested to just wanting to solve.

In one of the latest contributions to make the co-production idiom fruitful for studies in International Relations (IR), Lindskov Jacobsen and Monsees introduce a very helpful understanding of co-production in its twofold process. They suggest studying the production *of* technology and the production *by* technology (Lindskov Johansen and Monsees 2019, 26). With the production *of* technology they focus on the analysis of the various social practices and discourses that contribute to the social production of scientific facts and technological authority (27). The perspective on the social production *by* technology looks into the agentic capacity of technology itself. According to them, such an analysis highlights 'how sociotechnical formations loop back to change the very terms in which we human beings think about ourselves and our positions in the world' (Lindskov Johansen and Monsees 2019, 29).

Going back to our material with a focus on the co-production idiom then means to trace moments and expressions in which identities, problems and their solutions are produced and how the agency of entities, be it human or non-human ones, is an outcome of social practices and processes (Lindskov Johansen and Monsees 2019, 36). Lior Weiss (name

changed), another security expert attending the conference, opened his laptop during our interview and presented his computer-based simulation to us. In this simulation, Weiss and his colleagues are able to model and visualise any possible catastrophic scenario in any possible city worldwide. Taking the observer through a vivid journey of skyscrapers, malls, concert halls and stadiums, Weiss can pause the simulation at any time and visualise any kind of threat that is not yet in the scenario but might possibly evolve. Instantly, Weiss can put up explosives next to a metro station, place snipers on rooftops or simulate movement next to a fully booked soccer stadium, being able to exactly measure the distance between possible perpetrator, threat and victims. Through this, the initially unharmed urban environment turns into a map of possible threats in which every urban infrastructure has the potential to become a site of attack and devastation.

As the simulation illustrates our case that not every infrastructure is critical but can be securitised and, in this way, determined to be critical. By helping possible customers to imagine a city as a cartography of possible threats that have not yet materialised, the 3D pictures of companies such as the one from Lior Weiss are virtually turning ordinary infrastructures into sites of destruction, rendering them visible as vulnerable spots that warrant protection. This materialisation of infrastructure as 'critical' in turn requires a specific expertise to accompany the process of its securitisation. The assessments of security experts who imagine and simulate potential threats are themselves '*generative* of policy problems' (Machold 2016, 14). They create the catastrophic imaginaries to which they then deliver their possible solutions.

The expertise and knowledge presented at the conference 'should not be understood as a resolution to a pre-given set of problems (technical, political or otherwise), but rather as a kind of policy diagnostic, which enacts realities that it claims to only describe and respond to' (id.). In co-production terms this entails to understand how critical infrastructure is produced as technology under threat. At the same time, the infrastructure that evolves as threatened in front of our eyes becomes productive in a sense that it requires further expertise, knowledge and technologies to be assembled in order to be secured. The need for expertise and technology is inflated by technology itself.

Teaching what's critical – the (co-)production of public and private expertise

> The experts have to do the teaching to the municipalities. This (teaching) should come from the industry, the companies. Sometimes we (the industry) have to force them, to teach them and bring professional companies in order to bring partners for a solution. First, we begin with education of the municipality and also the cities (…) They have to put people in charge. Then we begin the implementation of the system and action, depending on defining what infrastructure is critical.[6]

By mentioning the role of private security companies in the process of 'teaching' municipalities and other state bodies about their potentially critical infrastructure, Itai Davidi (name changed) describes two entangled notions of the co-construction perspective: first, his statement clearly indicates the process-character of producing infrastructure as critical. By mentioning that the implementation of any system of action depends on what infrastructure gets to be defined as critical, Davidi points to the productivity of this process: As security companies are not only providing the solutions to existing

problems but are productive of the problems that they then offer solutions for, these companies are part of producing critical infrastructure.

Second, Davidi's statement reflects the that the role of private security companies is far from providing solutions to a domain in which the state defines and controls matters of security. According to Davidi, private security firms take initiative and even force municipalities to understand and learn about their potentially critical infrastructure. As a result of this interaction, private and public security actors become constituted. They are attributed certain knowledge and certain tasks. They are not separate entities that pre-exist to their actions but rather come into being through these actions.

Thus, in line with our co-production argument, what we find in the material is that private and public actors are mutually constitutive: in many forms of cooperation, actors relate to each other and the other's potential interests, thereby producing the demands they then willingly serve. At the conference, a conversation with two security professionals illustrates this relation very vividly. Both male professionals had left the military after completing over 20 years of service in the ranks of colonel and major. From their long experience in the army, they had developed a very clear sense of the demands that the military directs at the private sector. Asked what drives their work and the development of security technology, in this case drones, they responded:

> It's coming from needs. I'm coming from the air force and I used to fly UAV [unpiloted aerial vehicle]. And he [points to his colleague] is coming from other fields of the army, intelligence for example. So after all, the military have their needs, they want very small things, very smart things, very fast. (…) They just prefer to buy. The Israeli army is buying. It's not developing. Look, in Israel there is a lot of industry (…) the army is saying: why should I be a manufacturer? (..) In the end of the day, the price is gonna be cheaper. After we develop for the army or the police system we realise that a lot of inquiries [come] from other sections.

This statement provides insights into the close entanglements, even forms of dependencies, that take shape in forms of cooperation between public and private actors. Israeli security professionals who had previously served in the army and are now working in the private sector know exactly the needs and demands of the public sector. They specifically develop and manufacture their products for the public sector, the Israeli Defense Forces in this case. As such, private security firms do not only function as service providers to the defined security challenges of public institutions nor do they just assess and define risks and threats. They literally produce what they anticipate the public sector to be wanting. This form of co-construction is not the result of a problem that the state and its different actors define in order to seek help in the private sector. Instead, problematisations of public security derive from interactions between firms and authorities in which what counts as 'public' becomes constituted in the first place.

The co-production of security for digital infrastructures

The close relations between the Israeli military and the country's economy have lately gained increased prominence with regard to one specific field – cyber security. It was a common sense at the conference that this field will gain importance in the near future, and Israel was portrayed as being at the forefront of this development. The country is already seen as one of the main drivers of cyber security advancement. The reason for this is, again, the close cooperation of the Israeli military and private sector. The most

prominent example is *Unit 8200* within the IDF which is surrounded by rumours and stories on its covert activities. The unit has attracted attention for its secret military operations, but also for its transfer of knowledge into the private sector as its former members regularly leave the IDF to start their own business, many in the field of cyber security (Reed 2015). For example, the *Financial Times* has described the unit as 'the Israeli military's legendary high-tech spy agency, considered by intelligence analysts to be one of the most formidable of its kind in the world', adding an expert statement that describes the country's efforts within the field as existential, 'Israel needs to be excellent in cyber. We are getting attacked again and again – our banks, our critical infrastructure, our government'.

These motives have also been reiterated by an interviewee at the conference who works within the cyber-security domain. Parts of his statement have been used in the introductory quote. The following provides the broader context in which he relates the military experience to the way how security as well as economic problems are tackled:

> Being Israeli and surrounded with Arab nations, partly enemies, we're always kind of thinking ahead. We're very proactive, trying to figure out what's gonna happen next. How can I know if that happens, what should I do? We're kind of building these defences and thinking … We think proactively and we're ahead, we're risk takers. (…) Just living in Israel, that's what it does to you.[7]

This quote speaks to a number of aspects that indicate how strongly experiences within the public and private realm are connected within the Israeli context. The interviewee connects the military experience to a specific attitude of the Israeli security culture which is seen to enable them to thrive in the business world. He implies that it would be a similar kind of risk-taking attitude that would enable former Israeli soldiers to thrive in the business environment – coming out of the army would enable them to become the 'next Mark Zuckerberg'.

The field of digital infrastructure security presents a most interesting case to assess the intersections of public and private efforts in the securitisation of infrastructure. Unlike in other infrastructural domains, within the digital sphere the provision of security has not been handed from public to private actors because 'cyber security' has hardly ever been a domain of the state. The provision of cyber security appears to be a constant struggle between public and private actors, more precisely: it appears as a symbiosis of both, a very concrete case of co-production. As indicated above, speaking of 'commercialization' of digital security would be misleading as private actors originally developed many security practices while state actors have only been adapting them.

Although public authorities and security forces have been 'catching up' in many regards, private actors develop and maintain most digital infrastructures. They provide expertise and methodologies that define possibilities and threats. As this field of security has gained growing attention within the last years, the state has also increasingly sought to expand its capabilities. Attempts to 'securitize' the topic include a number of referent objects: threats to private companies, to citizens and their privacy, and also to nation states. Already in 1998, there have been attempts by the military to securitise the cyber and thereby claim authority to oversee this sphere (Buzan, Wæver, and de Wilde 1998). While these aspirations were not fulfilled at that time, discourses concerning 'cyberspace' are filled with attempts to frame and highlight certain threats and future risks. Hence, a

number of actors compete in their demands aiming to define and defend cyber-security (Balzacq, Leonard, and Ruzicka 2016).

While initially enthusiasm of the possibilities of the data superhighway prevailed, it became a concern of the military and intelligence sector due its lack of (state) control. The political emphasis shifted from how to build and expand the digital infrastructure towards questions on how it should be secured (Schulze 2017). Such concerns included the two facets securing infrastructures that have been introduced above: the security of the cyber as well as security through cyber (Betz and Stevens 2013). Considering the close entanglements of public and private efforts in the development of digital infrastructure, it can be described as a co-production while the product itself, the global digital infrastructure, challenges notions public and private. Cyber-security thus unites a range of at least partly paradoxical demands and thereby constitutes a reference object which Marieke de Goede and Stephanie Simon have described as 'unmappable in its entirety and unknowable in its essence' (2015, 89). As a consequence, cyber-security itself presents a means to address these manifold claims. Tim Stevens (2016, 2) explains, 'cyber security is a response to the perceived risks and threats of the modern, global information-technological infrastructure most commonly glossed as 'the internet'. In broad terms, it is concerned with anyone and anything that communicates through digital, electronic means'.

Unsurprisingly, the provision of this world-wide communications infrastructure has also been characterised as 'critical'. In Israel, the *Security in Public Bodies Law* of 1998 gave public bodies increased authority of supervision. Remarkably, the regulation of public bodies includes over a dozen of public and civilian organisations as well as firms (Tabansky 2013). Acknowledging these entanglements, we can understand public demand for security and economic logics as constitutive for each other within the digital sphere. However, the interactions of public and private actors may have controversial effects. Some software companies also have the ability to do offensive cybersecurity, meaning the skills to enact surveillance via digital devices. An Israeli company that is tightly linked to the above-mentioned Unit 8200 has been accused of helping authoritarian governments to hack phones of journalists and human rights workers (Timber and Greene 2019). The complex dynamics between differing states, their authorities, private companies and civil society within the field of cyber security have become a topic of ongoing public discussions within the last years, most certainly after the Snowden revelations (Bauman *et al.* 2014). While state actors rely on private services in their surveillance of large parts of online communication, they also exploit weaknesses in these private security architectures to enable targeted operations. These constellations show that both state and private actors play ambiguous roles within the field of cyber (in-)security.

Conclusion

This contribution has put forward the concept of co-production to account for the close entanglements of public and private actors within the sphere of infrastructural security. As our empirical insights have shown, the lines between the sectors at times blur, they are constantly re-negotiated and re-drawn. Actors change sides and seamlessly take on new roles within the public as well as within the private realm. The securitisation of infrastructure appears as a joint public-private endeavour in which both sides fulfil specific tasks and direct expectations and demands towards the other. However, the distinction

between the public and the private cannot be overruled altogether as Neocleous (2007) suggests. Rather, we need to better account for the varying dynamics that are engendered by these forms of co-production as well as possible contradictions.

Although public-private cooperation and co-constitution are driving forces within the field of infrastructural security, it would be misleading to assume an uncontested alliance. Reclaiming the dividing line between both fields can be constitutive of agency on both sides. While state actors may demand efficiency and innovation from the private sphere, the private sphere expects the state to provide the frameworks to conduct business. As indicated above, such attributions depend on the liberal division of state and market which has been re-affirmed within securitisation theory which sees the economy as a possible referent object, but less as an actor within securitisation itself (Buzan, Wæver, and de Wilde 1998). Our findings suggests that research into securitisation needs to take seriously the effects that stem from this division in the first place, not in order to disregard it altogether, but to understand the political implications that are engendered by these seemingly unpolitical sites of securitisation. Such an approach would take seriously the political economy of securitisation and underscore that there is no such thing as depoliticised security.

As the empirical insights have shown, distinctions between the two spheres are drawn by actors themselves and have an enabling effect. This is the case for those security professionals who are leaving the public sector in order to develop surveillance technologies. As former employees of the state, they have in-depth knowledge of the needs, standards and challenges of the public sector when it comes to issues of security provision. On the other hand, the public sector, in its multiplicity from the national to the regional and local level, is in need of sources of security provision amidst an ever-increasing broadening of security concerns. This is especially the case with regards to critical infrastructure since 'the potentially wide-range of civilian-infrastructure which might be deemed 'critical (…) signifies a move towards a much broader national security paradigm' (Steele, Hussey, and Dovers 2017, 79).

However, there are also differences between the two spheres that cannot be described as co-productive or mutually reinforcing. For example, the public and private field have very different forms of accountability. Generally speaking, in economically developed states, companies have to satisfy investors whereas public actors can be held responsible in differing forms if their form of government implies division of power. Also, depending on the institution and scale of its responsibilities, the state and its agencies might take much longer to not only plan, but also democratically legitimate specific projects.

In addition, contradictions can appear not only between private and public actors, but also between and across different state actors as well as between private actors. By discussing the interactions between public and state actors, we do not want to suggest that these fields can be treated as homogeneous entities. As the state cannot be grasped as one actor, let alone as a single entity with one will, diverging interests can occur in which contradictions and frictions become visible. From the national to the local level, political administration and responsibility are scattered and shared between different state agencies to which different tasks can be assigned. Infrastructure investment, let alone infrastructure maintenance, remains a blurry field of shared responsibilities of different actors. The same applies for the private sector which is even more heterogenous and diversified in small companies and international cooperation with very different forms of governance, labour, governance and organisation.

Throughout this paper, we suggested that the distinction between public and private actors as two separate and distinct entities engaging in security practices should be subject to intensified scholarly scrutiny. Rather, their relation should be analysed as potentially co-productive, shaping their identities and interests in processes of securitisation. The co-production perspective might thus be fruitful to study the complex and entangled processes in the field of security. Especially for those interested in the entanglement of expertise, materialities and technologies, a co-production perspective offers conceptual and methodological tools for further research.

Notes

1. See https://elnetwork.eu/country/israel/safe-smart-city-conference/
2. This only applies to Jewish and Druze citizens of Israel. Arab-Palestinians, who make up around 20% of the citizens of Israel, are not conscripted to the Army.
3. Interview, Safe and Smart City Conference, November 19th, 2018.
4. See https://www.safeandsmartcity.org/, last accessed December 9th, 2019.
5. Interview number 3 with Tomer Avishai, Safe and Smart City Conference, November 19th.
6. Interview, Safe and Smart City Conference, November 19th.
7. Interview, Safe and Smart City Conference, November 19th.

Acknowledgements

The authors would like to thank the two anonymous reviewers for their instructive comments. This paper has also greatly benefitted from Andreas Langenohl's most helpful comments and Johannes Gunesch's valuable feedback and careful reading. Amina Nolte's research was carried out within the collaborative research centre 'Dynamics of Security' /Transregio 138 at the Justus Liebig University Giessen and Philipps University Marburg. Carola Westermeier's work was carried out in the framework of the research project 'FOLLOW: Following the Money from Transaction to Trial',

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

Carola Westermeier's work was carried out in the framework of the research project 'FOLLOW: Following the Money from Transaction to Trial', funded by the European Research Council, Grant No. ERC-2015-CoG 682317.

References

Abrahamsen, Rita, and Anna Leander. 2016. "Introduction." In *Routledge Handbook of Private Security*, edited by Anna Leander and Rita Abrahamsen, 1–8. London: Routledge.

Abrahamsen, Rita, and Michael C. Williams. 2009. "Security Beyond the State: Global Security Assemblages in International Politics." *International Political Sociology* 3 (1): 1–17.

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

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

Avant, Deborah. 2005. "Private Security Companies." *New Political Economy* 10 (1): 121–131.

Balzacq, Thierry, Sarah Leonard, and Jan Ruzicka. 2016. "'Securitization' Revisited: Theory and Cases." *International Relations* 30 (4): 494–531.
Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B. J. Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8 (2): 121–144.
Betz, David J., and Tim Stevens. 2013. "Analogical Reasoning and Cyber Security." *Security Dialogue* 44 (2): 147–164.
Burgess, James Peter. 2007. "Social Values and Material Threat: The European Programme for Critical Infrastructure Protection." *International Journal of Critical Infrastructures* 3 (3/4): 471–487.
Buzan, Barry, and Ole Wæver. 2003. *Regions and Powers. The Structure of International Security*. Cambridge: Cambridge University Press.
Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner.
Callon, Michel. 1984. "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay." *The Sociological Review* 32 (1): 196–233.
Collier, Stephen J., and Lakoff Andrew 2010. "Infrastructure and Event. The Political Technology of Preparedness." In *Political matter. Technoscience, democracy, and public life*, edited by Bruce Braun and Sarah Whatmore. Minneapolis: University of Minnesota Press.
de Goede, Marieke. 2012. *Speculative Security: The Politics of Pursuing Terrorist Monies*. Minneapolis: University of Minnesota Press.
de Goede, Marieke. 2018. "The Chain of Security." *Review of International Studies* 44 (1): 24–42.
Engels, Jens Ivo. 2018. *Key Concepts for Critical Infrastructure Research*. Wiesbaden: Springer Fachmedien.
Folkers, Andreas. 2017. "Existential Provisions. The Technopolitics of Public Infrastructure." *Society and Space* 35 (5): 855–874.
Folkers, Andreas. 2018. "Was ist kritisch an Kritischer Infrastruktur? Kriegswichtigkeit, Lebenswichtigkeit, Systemwichtigkeit und die Infrastrukturen der Kritik." In *Was heißt Kritikalität? Zu einem Schlüsselbegriff der Debatte um Kritische Infrastrukturen*, edited by Jens-Ivo Engels and Alfred Nordmann, 123–154. Bielefeld: Transcript.
Graham, Stephen, and Alexander Baker. 2016. "Laboratories of Pacification and Permanent War: Israeli-US Collaboration in the Global Making of Policing." In *The Global Making of Policing: Postcolonial Perspectives*, edited by Jana Hönke and Markus-Michael Müller, 40–58. London: Routledge.
Grassiani, Erella. 2018. "Between Security and Military Identities. The Case of Israeli Security Experts." *Security Dialogue* 49 (1-2): 83–95.
Halper, Jeff. 2015. *War Against the People: Israel, the Palestinians and Global Pacification*. London: Pluto Press.
Harbers, Hans. 2005. "Epilogue: Political Materials – Material Politics." In *Inside the Politics of Technology. Agency and Normativity in the Co-Production of Technology and Society*, edited by Hans Harbers, 257–272. Amsterdam: University Press.
Harvey, Penny, Casper Bruun Jensen, and Atsuro Morita. 2017. *Infrastructures and Social Complexity: A Companion*. London: Routledge/Taylor & Francis Group.
Hayes, Ben. 2014. "The Surveillance-Industrial Complex." In *Routledge Handbook of Surveillance Studies. Routledge International Handbooks*, edited by Kirstie Ball, Kevin D Haggerty, and David Lyon, 167–175. Abingdon: Routledge.
Hever, Shir. 2018. *The Privatization of Israeli Security*. London: Pluto Press.
Hoijtink, Marijn. 2014. "Capitalizing on Emergence: The 'New' Civil Security Market in Europe." *Security Dialogue* 45 (5): 458–475.
Itai, Davidi. name changed. *Personal Interview*. Safe and Smart City Conference Jerusalem, 19 November 2018.
Jasanoff, Sheila. 2004. "Ordering Knowledge, Ordering Society." In *States of Knowledge: The Co-Production of Science and Social Order*, edited by Sheila Jasanoff, 13–45. New York: Routledge.
Joachim, Jutta M., and Andrea Schneiker. 2018. *Private Security and Identity Politics: Ethical Hero Warriors, Professional Managers and New Humanitarians. Routledge Private Security Studies*. London: Routledge/Taylor & Francis Group.

Knoblauch, Hubert. 2005. "Focused Ethnography." *Forum Qualitative Research* 6: 3. http://www.qualitative-research.net/index.php/fqs/article/view/20/43#gcit.
Krahmann, Elke. 2008. "Security: Collective Good or Commodity?" *European Journal of International Relations* 14 (3): 379–404.
Krahmann, Elke. 2018. "The Market for Ontological Security." *European Security* 27 (3): 356–373.
Lakoff, Andrew, and Stephen Collier. 2010. "Infrastructure and Event. The Political Technology of Preparedness." In *Political Matter: Technoscience, Democracy, and Public Life*, edited by Bruce Braun and Sarah J. Whatmore, 243–266. Minneapolis: University of Minnesota Press.
Langenohl, A. 2019. "Dynamics of Power in Securitization: Towards a Relational Understanding." In *The Power Dynamics of Securitization: From the Early Modern Period until the Present*, edited by Andras Langenohl and Regina Kreide, 19–55. Baden-Baden: Nomos Verl.-Ges.
Leander, Anna. 2005. "The Market for Force and Public Security: The Destabilizing Consequences of Private Military Companies." *Journal of Peace Research* 42 (5): 605–622.
Leander, Anna. 2010. "Commercial Security Practices." In *The Routledge Handbook of New Security Studies. Routledge Handbooks*, edited by J. Peter Burgess, 208–216. London: Routledge.
Leander, Anna, and Rens van Munster. 2007. "Private Security Contractors in the Debate About Darfur: Reflecting and Reinforcing Neo-Liberal Governmentality." *International Relations* 21 (2): 201–216.
Lindskov Johansen, Katja, and Linda Monsees. 2019. "Co-Production: The Study of Productive Processes at the Level of Materiality and Discourse." In *Technology and Agency in International Relations*, edited by Matthias Leese and Marijn Hoijtink, 24–41. London: Routledge.
Lyon, David. 2009. *Surveillance, Power, and Everyday Life*. Oxford: University Press.
Machold, Rhys. 2016. "Learning From Israel? '26/11' and the Anti-Politics of Urban Security Governance." *Security Dialogue* 47 (4): 275–291.
Neocleous, Mark. 2007. "Security, Commodity, Fetishism." *Critique (Clandeboye, Man)* 35 (3): 339–355.
Nolte, Amina, and Ezgican Ozdemir. 2018. "Infrastructuring Geographies: Histories and Presents in and of the Middle East and North Africa." *META – Middle East – Topics & Arguments* 10: 5–20.
Reed, John. 2015. "Unit 8200: Israel's Cyber Spy Agency." *Financial Times*, 10 July. https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c.
Schulze, Matthias. 2017. *From Cyber-Utopia to Cyber-War. Normative Change in Cyberspace*. Unpublished PhD thesis, Friedrich-Schiller-Universität Jena.
Simon, Stephanie, and Marieke de Goede. 2015. "Cybersecurity, Bureaucratic Vitalism and European Emergency." *Theory, Culture & Society* 32 (2): 79–106.
Steele, Wendy, Karen Hussey, and Stephen Dovers. 2017. "What's Critical About Critical Infrastructure?." *Urban Policy and Research* 35 (1): 74–86.
Stevens, Tim. 2016. *Cyber Security and the Politics of Time*. Cambridge: Cambridge University Press.
Stockmarr, Leila. 2016. "Beyond the Laboratory Thesis: Gaza as Transmission Belt for War and Security Technology." In *The Global Making of Policing: Postcolonial Perspectives*, edited by Jana Hönke and Markus-Michael Müller, 59–76. London: Routledge.
Tabansky, Lior. 2013. "Critical Infrastructure Protection." *International Journal of Cyber Warfare and Terrorism* 3 (3): 80–87.
Timber, Craig, and Jay Greene. 2019. "WhatsApp Accuses Israeli Firm of Helping Governments Hack Phones of Journalists, Human Rights Workers." *The Washington Post,* October 29. https://www.washingtonpost.com/technology/2019/10/29/whatsapp-accuses-israeli-firm-helping-governments-hack-phones-journalists-human-rights-workers/.
Tomer, Avishai. name changed. *Personal Interview*. Safe and Smart City Conference Jerusalem, 19 November 2018.
Volinz, Lior. 2018. "Governance Through Pluralization. Jerusalem's Modular Security Provision." *Security Dialogue* 49 (6): 438–456.
Wakefield, Stephanie. 2018. "Infrastructures of Liberal Life: From Modernity and Progress to Resilience and Ruins." *Geography Compass* 12 (7): 1–14.
Weiss, Lior. name changed. *Personal Interview*. Safe and Smart City Conference Jerusalem, 19 November 2018.