SECURITY DIALOGUE

Article

Security Dialogue
2021, Vol. 52(3) 231–248
© The Author(s) 2020
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/0967010620933513
journals.sagepub.com/home/sdi
SAGE

Automating security infrastructures: Practices, imaginaries, politics

Nathaniel O'Grady
University of Manchester, UK

Abstract

This article contributes to emergent debates in critical security studies that consider the processes and effects that arise where new forms of automated technology begin to guide security practices. It does so through research into public Wi-Fi infrastructure that has started to appear across the globe and its mobilization as a device for warning the public about emergencies. I focus specifically on an iteration of this infrastructure developing in New York called LinkNYC. According to the infrastructure's operators, the processes that underpin emergency communication have gradually become 'automated' to accelerate LinkNYC's deployment during crises. The article pursues three lines of inquiry to explore the automation of security infrastructure, in turn making three correspondent original contributions to wider debates. First, it unpacks the real-time analytics and platform-based data-sharing techniques cultivated to automate emergency communication. Here, I expand understanding of the new forms of automation now integrated into technologies harnessed for security and their practical effects. These forms of automation, I demonstrate secondly, are situated by those governing into wider imaginaries concerning the transformative promise automation bears. I argue that the proliferation of these imaginaries play a crucial role in justifying and dictating the enrolment of new devices into security. Third, it explores how automation affords private companies the opportunity to exercise discretionary decisionmaking that changes how and when infrastructure should operate during emergencies. Developing this argument, I add new dimensions to debates regarding the political ramifications associated with automation by claiming that automation redistributes authority across the public and private organizations that increasingly coordinate in bringing new technologies to bear in the security domain.

Keywords
Algorithmic governance, automation, discretionary decision, infrastructure, public–private hybrid, security

Introduction

From border security (Hall, 2017) and counter-terrorism (Leese, 2014) to predictive policing (Brayne, 2017) and finance (Campbell-Verduyn et al., 2017; MacKenzie, 2019), the issue of automation and algorithmic governance is now a cornerstone of critical security studies research that probes the myriad intersections between security practices and data-based technologies.[1] In recent times, this

Corresponding author:
Nathaniel O'Grady, University of Manchester, Ellen Wilkinson Building, Oxford Road, Manchester, M13 9PL, UK.
Email: nathaniel.ogrady@manchester.ac.uk

work has begun to operate on the basis that, owing to technological change, automation encapsulates a more expansive set of computational processes than previously assumed. Rather than simply referring to rules-based algorithmic instructions dictating the operation of technologies that proceed without human intervention, automation functions through complex relations with the broader circumstances in which it is situated. As elaborated in the next section, automation is actively shaped by these circumstances in various ways while also feeding back to actively affect them (Amoore, 2019; Aradau and Blanke, 2015, 2018; Bellanova and González Fuster, 2019; boyd and Crawford, 2012; Hayles, 2017; Hui, 2019; Leese and Hoijtink, 2019; Parisi, 2019; Ziewitz, 2016). And with the reconceptualization of automation, new forms of critique have developed to address the presence of automated technologies in security and the effects they bear. Automation has, for instance, been associated with the insertion of new rationalities (MacKenzie, 2011; Mirowski, 2014) and ontologies (Chandler, 2018) into security. In addition, automation transforms the grounds on which security agencies take steps to attend to risks, with algorithmically structured real-time analytics superseding statistically mediated renditions of population norms to encourage particular courses of intervention (see Hayles, 2012; Roberts, 2019; Rouvroy and Berns, 2013). Further still, arguments have developed concerning how automation sequesters government routines (Leese, 2014), weakens the accountability of public authorities (Laurauilt and Francoli, 2017) and extracts security decisionmaking from the realm of political contestation (Aradau and Blanke, 2015).

Contributing to this literature, this article investigates the security applications that are emerging with the development of the new public Wi-Fi infrastructure that is gradually making an appearance in cities across the world. Reflecting on interviews with a number of local government officials and representatives of the private companies subsidizing it, the article offers insight into a version of this infrastructure growing steadily across New York City in recent times, called LinkNYC or Link. This infrastructure acts as a security device because it has been adapted and deployed to communicate with the public about emergencies that the city experiences as both future risks and real-time events. I pay particular attention to how LinkNYC's security applications have, according to its operators, become automated over time to speed up its operation in times of emergency.

LinkNYC is important to consider because of its wider reverberations for ongoing debates that grapple with the role and effects born where new forms of automation shape and facilitate security practices. To ascertain its broader significance, the article approaches LinkNYC through three lines of inquiry, each of which makes a distinct contribution to existing research. I investigate, first, the cultivation of new data-sharing mechanisms and calculative logics that enable Link's translation into an automated emergency communication infrastructure. Link's salience here lies in how it develops further our understanding of the range of practices, constitutive of new forms of automation, that are now enrolled into security devices and the effects they generate upon the interventions that security agencies make (Amoore and Piotukh, 2015; Aradau and Blanke, 2015, 2018). Second, I explore how security practitioners imagine automation in terms of the transformative benefits it delivers (Leese, 2019). Leaning on Karan Barad's (2007) notion of materialization, I develop a distinct approach for conceptualizing these imaginaries, arguing that it is crucial to reflect upon them because they play a pivotal role in justifying the integration of new technologies into the security domain. The mobilization of automated technologies as security devices, to be clear, hinges in part on their promotion through, and infusion with, practitioner imaginaries concerning automation and the changes it may bring. And, lastly, the article examines how automation enables the private companies behind Link to exercise discretionary decisionmaking in determining when and how the infrastructure is used during emergencies. Unpacking discretionary decisionmaking, I establish fresh directions for critical analyses regarding the political effects that arise with automation. I claim specifically that automation raises new and significant issues concerning the distribution of authority across the public–private organizational partnerships that increasingly collaborate to enact security (Amoore, 2013; De Goede, 2012; Hoijtink, 2014).

The article proceeds through six sections. The first expands on pioneering literature stemming from critical security studies and beyond that has steered reconceptualizations of automation in recent times. In the next section, I situate these debates within research that reflects on the prominence of private companies where technological development facilitates security practices. I then turn specifically to LinkNYC, first describing the context in which its security applications have emerged. The article then analyses how automated practices infuse with practitioner imaginaries around automation to transform the infrastructure into an emergency communication device. Subsequently, I consider the political effects automation bears, demonstrating how it paves the way for discretionary decisionmaking and consequently instigates reappraisal of the distribution of authority amidst the public and private agencies now collaborating behind so many security technologies. The conclusion summarizes the article's arguments before extending debate further by offering trajectories for future investigation into the entanglement of security with advances in automation.

Automation reconsidered

Arising from debates in critical security studies and further afield, conceptualizations of automation as a set of computational processes integrated into digital technologies are currently undergoing serious reconsideration. Framing its existence beyond processes confined within software and code, this growing body of work claims that automation should be understood through the various and fluctuating relations it holds within the broader circumstances in which it is situated. This framing of automation as relational appears in many forms. With regard to security, we might direct our attention initially to the calculative logics through which computational technologies now make sense of data critical for understanding risks. The pioneering work of Louise Amoore (2019), Luciana Parisi (2019) and Yuk Hui (2019), for example, implores scholars to think of automation, as well as the algorithms that underpin it, in a way above and beyond its incarnation within deductive logics that execute prescribed rules to render intelligible structured datasets that contain data that have already been collected and classified. Excavating logics associated with the term *machine learning*, through which algorithms rewrite their own rules to keep making sense of real-time data, the authors show instead that automated devices develop in tow with the indeterminate and emergent situations they address. While logics themselves are pivotal, scholars have also rethought automation on other trajectories.[2] The forms of automation that machine-learning logics usher in, Claudia Aradau and Tobias Blanke (2015) argue, would not possess such consequence were it not for legislative changes that reshape, for example, the harvesting of data in the first place. Further still, Luca Introna (2016) observes that automation results from a reconfiguration of relations between material devices such as online platforms to enact new data-sharing procedures.

But shaped by its relations to ever unfolding circumstances, automation also appears across debates as a labelling device through which to afford meaning to technological processes. Research thus urges consideration of the mythologies or imaginaries that ensconce and surround automation in the security domain. Carrying with them 'entrenched assumptions about the politics of computation, automation, and control' (Ziewitz, 2016: 4), these imaginaries are historically and culturally situated renditions concerning what automation is, the capabilities it expresses and the promises it holds (Balsamo, 2011; Gillespie et al., 2014).[3] These imaginaries, however, strike an ambiguous relationship to the technical practices and material devices with which they purport to correspond. Following Lucy Suchmann, Mathias Leese (2019) elaborates on the concept of configuration to render scrutable how such imaginaries develop through the design of security technologies that, in their execution, reproduce and proliferate modernist delusions of human mastery. While Anne Balsamo sees these imaginaries as co-produced amid the ongoing negotiations that characterize the relationship between humans and their technological counterparts,[4] M. C. Elish and danah boyd (2018: 58) claim conversely that 'dominant conceptions of how Big Data and AI work do not align with the actual techniques of machine learning'.[5,6] Despite their variant rapport with the technological materialities they represent, such imaginaries predominantly depict automation as increasing the speed of computational processes, streamlining banal organizational routines, creating 'objective' knowledge untarnished by human error and even manifesting omniscience (boyd and Crawford, 2012; Wajcman, 2019). In addition, these imaginaries map onto a catalogue of organizational sites, serving heterogeneous interests. At times emblematic of the overly optimistic commentaries of academics, they are also enlivened through the promotional literature of software developers and security agencies' justifications for expenditure on new resources (Elish and boyd, 2018; Lindskov-Jacobsen and Fast, 2019).

While developing in multiple ways through its intersections with broader circumstances, automation must also be conceptualized by what might be called its recursive performativity in relation to security. In other words, automation creates new effects within the security contexts in which it is inexorably interwoven (see also Balsamo, 2011; Introna, 2016; Leese and Hoijtink, 2019; MacKenzie, 2019; Matzner, 2019). Developing the notion of what she calls the 'automation of automation' to engage with algorithms that undergird machine-learning practices that feed off and attune with wider environmental stimuli, Luciana Parisi argues that 'it is evident today that the automation of automation . . . involves a cultural transformation in the *conceptualization* of reasoning with and through machine thinking' (Parisi, 2019: 94, emphasis added). She observes further that automation is 'not a formal apriori, but corresponds to the conceptual infrastructure of social practices' (Parisi, 2019: 97). Taking her lead from Katherine Hayles (2012), Parisi shows that the new cognitive capabilities surfacing with the development of artificial intelligence diffuse widely, interlacing with ways of thinking that permeate socially. Moreover, automation is supported by, and actively re-engenders, an array of social practices that develop in the sites into which it becomes embedded.[7]

For the specific purposes of the present article, the literature reviewed in this section impacts significantly on investigations into the presence of new forms of automation in security practices and their ramifications. It orients us towards a deeper consideration of the logics and material relations developed so that technological devices used for security can operate through new forms of automation. At the same time, it directs attention to how security practitioners imagine automation and the importance of their imaginaries in creating the conditions of possibility in which security devices become automated. But, by framing automation as performative, existing debates also open up to consideration the wider political effects felt with the integration of new forms of automation into security. To posit these effects within the context this article addresses, I now engage with critical security studies literature that confronts the role of private companies where security and technology interweave.

Situating automation amid public–private security hybrids

Although automation itself has yet to be considered in relation to it, the role of private companies is far from an alien notion in research that investigates the security–technology nexus. Existing arguments steer attention to how the rising influence of private companies derives from conditions in which data prove evermore pivotal in guiding and legitimating security practices. With the storage, circulation and analysis of various data crucial to their own business models, financial institutions, for example, find themselves increasingly responsible for tracking global monetary flows that might indicate possible associations between suspected terrorists (De Goede, 2012). Accumulating profit through the collection of vast amounts of user data, social media companies are also becoming increasingly serious about monitoring, identifying and reporting security threats (Lally, 2017). Simultaneously, however, government adoption of new security strategy paves the way for the increased prominence of private actors. Shifts in local municipal policy, exemplified by smart urbanism initiatives to which LinkNYC might be said to belong, bestow unprecedented authority upon a range of private firms like software designers, data-brokerage corporations and telecommunication conglomerates in shaping the way that cities are governed (Ayala and Marvin, 2015; Kitchin, 2014; McFarlane and Söderström, 2017; Mattern, 2014; Meijer and Bolívar, 2016).[8]

But developments in the design of technology itself, alongside the practices cultivated to bring technologies to bear, also enable the more pronounced role of private companies. Enterprising software developers have seized upon security problems as so many business opportunities for which to invent apparent technological solutions (Amoore, 2013). Analytics firms craft techniques to furrow deep within ever-unfolding streams of big data to analyse their significance for whatever goals their contractors pursue (Amoore and Piotukh, 2016), while designers have invented malleable software that finds new purposes as it is applied by end-users to meet different aims (Galloway, 2012; O'Riordan, 2017).

Scholars have gone further still, encouraging deep exploration of the specific forms of agency that private institutions enact, seize or are otherwise granted.[9] While some work stresses the new registers of power these firms appropriate (Williams, 2010), other studies have focused on how they perform and negotiate their new responsibility (De Goede et al., 2014). Investigations have pursued how the bearing that such companies exercise, and the type of influence they enact, is tied up with the transference and circulation of heterogeneous material things across the security domain. Alongside software, scholars have traced databases by their movement from one sector to another (O'Grady, 2018). But pursuing the movement of such objects might nevertheless bear witness to the somewhat surreptitious flow of other things entirely. Invoking what she calls the *chain of security*, Marieke de Goede details how information-exchange infrastructure spanning the globe integrates new forms of knowledge into security. A matter of ongoing repair, this infrastructure is tightly bound to, and actively re-produces, security knowledge that is 'continually modulating' (De Goede, 2018: 38). It is not only knowledge that attains new degrees of motility where 'public–private hybrids' (De Goede, 2012: 55) prevail, however. Such knowledge also entails new forms of action. Via the algorithms they write and sell, technology firms, according to Louise Amoore and Rita Raley (2017: 7), are 'involved in the making of actionable worlds', helping to mould the very modes of intervention by which security takes place. As their products and services become more important, then, private firms begin to weigh upon not only the forms of knowledge drawn upon by security organizations but also the actions and decisions characterizing security itself.

Critical security studies research also compels investigation of private firms' reliance upon the conjuring of risk-laden futures.[10] The unavoidable indeterminacy around future emergencies offers companies a unique selling point in their endeavours to win government contracts, meaning that 'uncertain futures are commodified' (De Goede et al., 2014: 419) as they consolidate as horizons towards which new forms of analysis and monitoring can be oriented (Amoore, 2013). For Marijin Hoijtink (2014), uncertainties concerning risks are deeply interwoven with the business models of private firms who seek to capitalize on the emergence that ever-pervades the world's remaking. But riskscapes are known, nonetheless, by their spatial coordinates as much as by their temporal referents. The array of private institutions enrolled into the security apparatus has increased with the growing recent popularity of the category of complex emergencies, a term that depicts events according to their cascading disruption as they course through interdependent components of infrastructure (De Goede et al., 2014; Zebrowski, 2019). While the lens of complexity renders risk a co-causal phenomenon, in which the effects of one disruption beget the causes of another, Torin Monahan and Neal Palmer's (2009) research into US Department of Homeland Security data fusion centres demonstrates that the conscription of multiple agencies, and their data, into the security apparatus can conflate and blur different kinds of threat.

This article brings these debates in critical security studies around public–private organizational hybrids into dialogue with those lines of inquiry concerning automation established in the previous section. While automation allows for critical exploration of the logics and imaginaries now organizing security technologies, the private–public security hybrids elaborated on by extant research open up to examination how the integration of automation into such technologies is guided through and conditioned by negotiations taking place between an array of security actors. The relations between public and private security actors provide the backdrop against which the article develops new arguments concerning the performative recursivity of automation. Situated amid the emergence of public–private hybrids, automation affects the distribution of authority for who decides how and when security technologies are deployed during emergencies. But, before turning to examine the automation of LinkNYC and delineating its effects for security, I offer a brief depiction of the context in which public Wi-Fi infrastructure has emerged in New York City, alongside its application in times of emergency.

LinkNYC and its deployment for emergency communication

When Mayor Bill de Blasio took to the streets of Manhattan in February 2016 to unveil LinkNYC in front of awaiting crowds and expectant media, it represented the culmination of a pivotal phase in the ongoing installation and development of one of the world's largest public Wi-Fi infrastructures. What would become known eventually as LinkNYC had its routes in De Blasio's 2012 pledge to expand all citizens' access to the internet, acknowledging the latter's importance as akin to other vital utilities such as water and energy (*NYC*, 2016). This pledge resulted in a publically issued request for proposals seeking companies to bid for the opportunity to oversee and bankroll the development and provision of public Wi-Fi infrastructure. Of the masses of proposals submitted, it was revealed in 2014 that the city government had granted the licence to design, install and operate this infrastructure to a conglomerate of private companies collectively known as CityBridge.

Although LinkNYC is composed in part of fibre-optic cables running through corridors stretching for miles underneath the city, its most visible manifestation is the 10-foot chrome kiosks that sit at street level. Each housing its own modem, these kiosks act as a Wi-Fi hub with a 150-foot range. On either side of the kiosks are 55-inch screens that beam adverts and announcements out onto the streets (see Figure 1).[11]

New Yorkers' reception to LinkNYC has been one of much contestation, with charges abound about heightened surveillance and claims that the infrastructure's installation violates health and safety regulations. Opposition groups have argued that CityBridge is simply using the city as a proof of concept or laboratory for a heretofore untested technology.[12] Local government authorities collaborating with CityBridge to coordinate LinkNYC, however, have strongly defended the project, pointing to the numerous public functions it serves.[13] The central focus of this article, one of these functions is that local government has been granted control of 5% of all content to be surfaced on Link screens. Along with announcements relating, for instance, to voter registration for elections and real-time updates on public transport, security agencies can use this screen time to deliver emergency communications should circumstances demand. As outlined in its Resiliency and Disaster Recovery Plan (DoITT, 2014), CityBridge will work with public authorities such as NYC Emergency

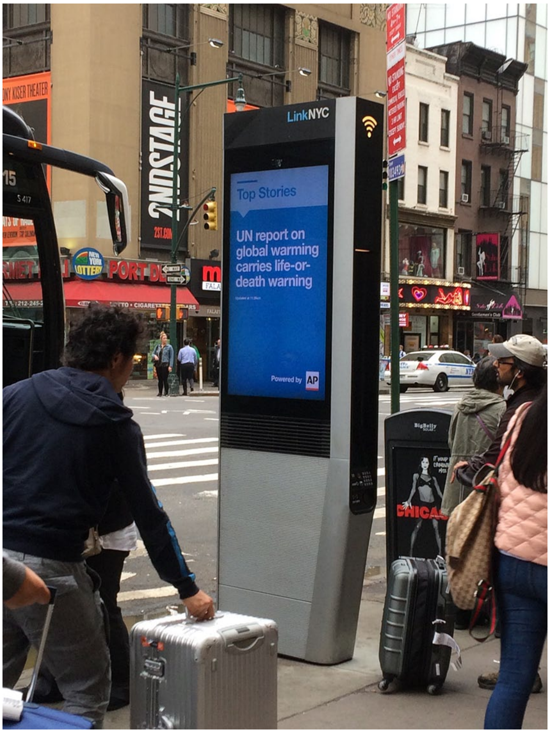

Figure 1. Example of a Link kiosk.
(*Source*: Author photo.)

Management (NYCEM)[14] and the New York City Department of Information Technology and Telecommunications (DoITT) so that messages flash up on Link screens warning the public about future adverse weather events that may prove disruptive. During the real-time unfolding of a wider array of emergencies, Link screens will advise the public about evacuation orders, shelter location and resources that might be required.[15] It is to the practices facilitating emergency communication, and their gradual automation, to which the article's attention now turns.

From 'manual' to 'automated' security infrastructure

Resonating with claims made in previous research imaginaries around automation are crucial to consider because they are fundamental in justifying the development of Link's security capabilities. But our understanding of these imaginaries and their significance can be extended by probing how they emerge and shape the actual technical practices through which technologies become automated. Automation imaginaries evidence processes that extend what Karan Barad (2007: 34) has referred to as 'materialization'. For Barad, materialization traces the course whereby a range of heterogeneous entities, be they human or non-human, come to take object status. Materialization is thus a means for capturing the progression through which an entity assumes and is bestowed a physical existence. In the case of this article, then, materialization would urge investigation of how automated security infrastructure comes into being through a range of technical processes. However, materialization also encompasses for Barad what she brands 'the causal relationship between discursive practices and material phenomena' (Barad, 2007: 34). Beyond accounting for the consolidation of a material entity, materialization encapsulates simultaneously the meaning that narrates its creation. Here, materialization allows for exploration of how security practitioners make sense of a technology's automation as it comes into being, along with the effects of this sense-making.

Taking a lead from Barad, I argue that automation imaginaries crystallize and manifest themselves in the implementation of new material devices for security purposes. However, in doing so, imaginaries also carry with them promises concerning how automation will change and improve the security practice it comes to underpin. Thus, imaginaries not only infuse into practices that automate security devices but also instantiate claims about the transformative potential automation bears, in turn justifying the integration of new forms of automation into security technologies. In Link, such imaginaries initially develop around practices that operators do not consider automatic and the limitations these practices place on the security applications of the infrastructure. While evoking the context in which Link emergency communication came about, one interviewee thus described how 'around the time we were getting this stuff going, the Chelsea bombing happened here in NY and that was a case . . . it was like, okay, one of these terrorist-related incidents, we set up just a manual Google form for them [Office for Emergency Management] to fill out and send to us'. At first, then, operators conceived of the practices underpinning emergency communication as existing in 'manual' form because of the kinds of informational exchange involved. Contrasting with pathways of exchange associated with big data, where interconnections between infrastructure enable voluminous data to be sourced and circulated to control rooms that appear as hubs within broader networks (Marvin and Luque-Ayala, 2017), a procedure developed in which city government would fill in and send to CityBridge a template. This template contained information relating to the perceived severity of the event, its likely effect on various infrastructural services, forecasts concerning its potential duration and guidance for the public about mitigatory steps to take. Sourced and transmitted by public authorities, Link operators projected the information onto screens throughout the city.

For Link's operators, the manual practices developed restricted the infrastructure's emergency communication capabilities.[16] Bearing semblance to Judy Wajcman's (2019) reflections concerning automation imaginaries, along with literature that outlines the entanglement of accelerationist discourses in the enfolding of digital devices into security more generally (Tanner and Meyer, 2015; Zebrowski, 2019), both local authorities and CityBridge criticized the manual practice described because of its slowness in disseminating information during an emergency. One operator narrated that 'given how this was kind of manual', emergency communication 'was going to take . . . a four-hour turnaround because you guys [NYCEM] have to let us know, we have to make sure our team manually sends this out to the right screens at the right time'. Describing NYCEM's reaction to CityBridge's proposal of a four-hour turnaround, they added that 'we kind of laughed because they were, like . . . our turnaround at NYC is, like, under two minutes. We, like, measure ourselves on the number of seconds it takes to get our message out.'

Stemming from this criticism concerning speed, imaginaries engender and legitimate the introduction of two new 'automated' processes that speed up the dissemination of information through Link during emergencies. First, for operators, automation was established by the cultivation of new information-sharing procedures ushered in through the reconfiguration of relations between data-sharing platforms existing across the different agencies behind Link. These new relations, second, enable analysis guided according to what Luciana Parisi (2019), after Charles Sanders Pierce, calls abductive reasoning.[17] In contrast to deductive logics that analyse structured datasets through rules-based algorithms, abductive reasoning continually generates new hypotheses and rules to make sense of data that reflect real-time circumstances as they unfold indeterminately.[18] The inauguration of these two new automated practices, however, also intimates towards the political effects that automation entails for the enactment of security through public–private hybrids. For Luca Introna (2016: 17), the performativity of the algorithms that form a crucial part of automation appears when they can be seen to operate as 'a prevalent mode of ordering and organisation'.[19] In other words, automation might renegotiate the practical arrangements across the organizations in which it is infused. Extending this argument, I show how with the routinization of new automated practices comes a redistribution of roles throughout the public–private organizational hybrid orchestrating emergency communications via Link.

Evidencing the new information-sharing procedures developed to move beyond what it describes as manual practices, CityBridge has established new means for remaining aware of emergencies. Operators describe these means as automated and requiring less exerted effort from public authorities.[20] Pertinent to research that unpacks the significance of platform media (Gillespie, 2010; MacKenzie, 2018), CityBridge now 'leverage[s] APIs' to gather data from open-source databanks. APIs – or 'application programme interfaces' – enable communication and the sharing of information between platforms that belong to different organizations.[21] CityBridge uses an API to access NYCEM's Rich Site Summary (RSS), a rolling log that contains communication data relating to all incidents to which city officials have been alerted. Data contained in the feed include the type of event, the source of the information, instructions that authorities have offered to the public and the time at which this information was communicated.

By leveraging APIs, CityBridge not only improves its access to, and oversight of, data circulating concerning events occurring across the city. In addition, and bringing to life the abductive reasoning that Parisi describes, the API also affords CityBridge an enhanced role, over and above that of local authorities, in analysing data and thus evaluating the emergency landscape. The API designed is ingestive. In their account of practices developed by security agencies to synthesize data from an array of social media platforms, Louise Amoore and Volha Piotukh (2015) capture how ingestion involves a double move that renders data amenable to analysis at the same time as they are being collected.[22] Rather than merely opening up data in their propriety, in other words, ingestion makes analysable all data that an organization can access. This includes structured datasets already indexically recorded, for instance, in spreadsheets like those found in Microsoft's Excel programme. But it also encapsulates yet to be classified and categorized unstructured data, which can be made sense of through 'the establishment of links with already indexed structured data and the creation of new indexes' (Amoore and Piotukh, 2015: 345). To interweave this ingestive-analytic capability into a process otherwise confined to data sourcing, Link operators have encoded a range of data triggers into their API. These triggers amount to prompts written into the API so that when particular information appears as the NYCEM RSS feed unfolds, inferences can be made that an emergency of a particular magnitude is either on the horizon or occurring. To take an example, one interviewee described how API leveraging meant that their colleagues 'got the message in that there was a heat advisory' issued by city authorities. Although only an advisory notice had been issued, it was inferred from the data that 'there was a potentially severe weather alert' for the city. Along with collecting data, the API thus makes it possible for CityBridge staff to execute their own calculative judgements concerning the possibility of a future serious emergency event.

An imagined shift to automation thus materializes in, and indeed justifies, the development of new technical practices for collecting and analysing data. However, and showing its initial recursive performative or recursive effects, automation also enacts two important transformations in relation to the delegation of tasks between different agencies. Private companies now take more responsibility for collecting the data that will steer the deployment of the infrastructure. In addition, these companies are also able to analyse that data to make sense of the city's indeterminate, ever-evolving riskscape with less input from public authorities.[23] In the next section, the article turns to consider the political effects that rise to the surface where automation redistributes the roles that public and private agencies play.

Discretion beyond the state

This section adds new dimensions to emergent claims about the political importance and effects automation bears for broader debates concerning the integration of technology into security practices. It does so by arguing that, alongside renegotiating the roles that they play, automation redistributes authority for who gets to determine how and when Link infrastructure is deployed for security purposes. This reconfiguration of authority is evident in the emergence and execution of discretionary forms of decisionmaking that change the thresholds for both activating the infrastructure in emergencies and dictating the content that it projects onto city streets. Both CityBridge employees and public officials described how, in their early exchanges with one another, they agreed clear criteria to determine when Link should be deployed and the content that Link screens should show. According to one interviewee, 'we sort of had to work together . . . to figure out what were the thresholds . . . where it was appropriate to put [emergency announcements] on screens'. These negotiations centred, they continued, on 'what can be shown and what should be shown and when, so . . . [CityBridge] can do it automatically' and thus without much oversight from public authorities. They explained further that 'there's classifications of level of emergency, and we decided to stick with the two top tiers', meaning that Link infrastructure would be mobilized when local authorities considered emergencies to be either severe or extreme.[24]

The announcements that appear on Link screens, nonetheless, often exceed these thresholds because CityBridge enacts discretionary forms of decisionmaking. Discretionary power has lineage in literature that unpacks the nuanced modes of decisionmaking packaged within contemporary security practices.[25] At one register, discretion captures decisions justified through response to matters of pressing and immediate circumstance, as opposed to compliance with the parameters of legally binding frameworks.[26] Accentuating how it 'combines the meaning of authority with the freedom to decide', Alexandra Hall (2017: 489) elaborates on discretion as thus both 'subjective and arbitrary – the antithesis of the liberal rule of law – raising concerns about inconsistencies and justice', but also as 'an ethical or humanizing device allowing abstract rules of law and policy to be justly applied to individual cases'. Although it bears the potential to instigate an array of ethical concerns through its exceedance of the law, one might conversely comprehend discretionary decisionmaking as a mechanism by which to adjust and accelerate governmental procedures in a manner sensitive to local needs.

The conditions of possibility for CityBridge to use discretionary decisionmaking are grounded in the redistribution of roles that automation affects. Once sourcing takes place through the leveraging of APIs detailed in the last section, CityBridge has access to all data that public authorities receive regarding incidents occurring across the city, affording it more licence in determining what data should be included in emergency communications. For instance, one interviewee depicted a hot summer's day on which the API indicated that emergency authorities had issued a heat advisory and subsequently arranged the opening of cooling centres containing air conditioning and water supplies strategically placed throughout the city. Although the opening of cooling centres itself breaches neither the severe or extreme incident category thresholds, emergency communications relating to them surfaced on Link screens. As one interviewee described:

> the cooling centres which were not, did not meet our severity criteria . . . [T]he fact that a cooling centre's opened is not a severe weather alert . . . [W]e got the message in that there was a heat advisory that was potentially a severe weather alert, which did trigger our feed, but we also saw value in . . . promoting the fact that cooling centres were open. So we can also use our *discretion* about how we can surface messages that might not meet our severity criteria but are also useful and actionable for constituents. (emphasis added)

Beyond data sourcing, the mobilization of abductive logics in analysis provides further grounds for the exercise of discretionary decisionmaking. In Hall's commentary, discretionary power appears where security practitioners interface with a computer screen to question and challenge what they see, so as to 'uncover the heterogeneity of life between data elements' (Hall, 2017: 497). Discretion, in Hall's incarnation, works to incorporate into security decisions the indeterminacies of life beyond computers that data cannot appropriately represent and code cannot process. In the case of Link, where operators leverage APIs to make sense of life in real time by tapping into ever unravelling RSS feeds, the relationship between data, analysis and discretionary decision is different. Where those abductive forms of reasoning outlined in the last section integrate into practice, more of the contingency that characterizes life, understood by Hall as beyond the computer, is accommodated because algorithms adapt in real time to make sense of broader contexts. In turn, Link operators feel able to report not only upon emergencies that actually appear but also on other events in the city that may be affiliated with them. With the integration of calculative logics emblematic of new forms of automation, discretion bears new effects where it guides the enactment of security through technology. Rather than disrupting the procedures established so that technologies can be deployed for security purposes, as in Hall's argument, discretion operates where abductive logics prevail to extend these procedures further, beyond that which has been agreed between public and private agencies.

Made possible because of the effects automation has on the distribution of authority for those coordinating Link and extending the presence of the infrastructure in emergencies, discretionary decisionmaking reflects a broader issue concerning the pervasiveness of public–private hybrids within and across the security apparatus. Bonnie Honig (2009) depicts an exemplary case of discretion by illustrating then Assistant Secretary to the US Department of Labour Louis F. Post's resistance to Federal Bureau of Investigation Director J. Edgar Hoover's legally sanctioned attempt in the 1950s to deport from the country thousands of people he suspected of being terrorists. For Honig (2009: 67), this case reveals discretionary power as a form of 'administrative agency' contained within the broader public sphere but residing beyond 'the more proceduralised domains of court and legislature'. Where discretion appears with Link, it does not symbolize the exercise of another form of decisionmaking facilitated through the complex compartmentalization of public governance into legal and administrative segments. Instead, private companies implement discretionary power while collaborating with public authorities. With their relationship orchestrated via new forms of automation, public-private hybrids evidence the enactment of discretionary decisionmaking beyond its oft-perceived parameters within the realms of the state, meaning that private companies assume new levels of authority for determining when and how security takes place.

Conclusion

Writing in 1990, Jonathan Crary laid out his investigation into the surfaces encountered in daily life. Including tabletops and mirrors, computer screens and the Earth's outer crust, Crary (1990) argued that surfaces exist as a point of singularity upon which multiple forces congeal. With its

55-inch screens located up, down and across Manhattan's grid and, to an ever-growing extent, New York's other boroughs, LinkNYC represents a collection of such surfaces. In recent times, the security applications of these surfaces have risen to prominence with communications flashing up on them warning the public of events that bear the potential to disrupt life as usual. This article, however, has sought to peel back the surface, to scratch underneath it and delve into the multiple practices and arrangements that, for the time being at least, make these emergency communications possible.

Tracing the gradual automation of LinkNYC's emergency communication capabilities, the article makes three contributions to ongoing debates that reflect on the significance of automation's role in, and effects for, the security–technology nexus. Engaging with literature from critical security studies and further afield that reconceptualizes automation beyond its reference to the execution of rules-based, black-boxed algorithms, the article, first, develops our knowledge of the practices constitutive of new forms of automation that increasingly underpin security technologies. But, second, it also establishes a distinctive approach to conceptualizing how security practitioners imagine automation. Such imaginaries are crucial to consider because, by envisaging the transformative benefits automation promises to bring, they justify the integration of new technologies into security practices. Lastly, the article expands upon the political effects that automation bears. Paving the way for private companies to act at their discretion in dictating the infrastructure's deployment, automation actively redistributes authority across the public–private hybrid coordinating Link. As an institutional configuration, public–private hybrids such as LinkNYC are increasingly commonplace with the further enrolment of automated technologies into governmental practice, and thus the new geographies of authority arising with them are vitally important for the future of politics of security.

The enactment of discretionary power in the private sector needs to be probed further by those exploring the intersections between technology and security. Such is the case for two reasons. First, new infrastructural projects and their security applications in neoliberal political economies, where public authorities have been stripped of funds to the extent that they are unable to operate independently, are from their inception always already privatized (see, for instance, Graham and Marvin, 2002; Silver 2017). Although motivated by the admirable goals of extending access to an increasingly vital resource in free Wi-Fi and developing new forms of emergency communication, it was always the case that a profit-oriented conglomerate would design, implement and operate New York's largest public Wi-Fi infrastructure. Second, various studies have claimed that legal and regulatory frameworks struggle to cope with the pace of technological change (Morozov, 2014). With the development of technology exceeding the capabilities of law-makers, discretionary power becomes part of the modus operandi of private companies who now take more control of the day-to-day running of security devices that, in order to continue functioning, necessarily exceed the legal parameters that supposedly provide the circumference for their development.

Enacted as a component of automated security infrastructure, the discretionary power of private companies also attains a level of mobility, being able to move across an increasingly exponential geographical space. As indicated by interviews conducted as part of this research, wider promotional literature and observation, Link networks have begun to expand throughout numerous cities on the eastern seaboard of the USA. Clusters of Links have appeared in cities across the UK too, from London and Glasgow to Manchester and Sheffield. Such an expansion confirms claims made across research into smart urbanism that cities operate as laboratories for technologies that, if successful, will take flight. What is less clear is whether another claim from the literature proves accurate with Link, namely, that many public service applications that the original 'lab' city were afforded in exchange for the instalment of infrastructure, including those related to security, do not make it to new cities (Evans, 2016; Kitchin, 2014). So long as the discretionary power of private companies proliferates, future research should investigate the continuities and discontinuities in the use of infrastructure for security and the political effects that appear as and when automated free Wi-Fi infrastructure spreads further across the world.

Acknowledgements

I am fortunate to have a supportive network of scholars around me who have offered generous and helpful critiques of previous drafts of this article as it has developed. My thanks extend to my fellow panellists and audiences in the sessions where I presented my research throughout 2019, including those at the Royal Geographical Society Annual Conference in London, the European International Studies Association Annual Conference in Sofia, the annual conference of the Italian Standing Group in International Relations in Trento and the Media of Cooperation conference in Siegen. I would also like to thank Mark Salter and the *Security Dialogue* editorial board, along with the two anonymous reviewers and John Morris, for their feedback and guidance on the final drafts of the article before its publication.

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Nathaniel O'Grady https://orcid.org/0000-0003-4400-7290

Notes

1. I use the term *automation* as opposed to *algorithms* or *algorithmic governance* throughout the article owing to the different scales of computation each term accounts for. Algorithms address the sequence of procedures written so that computation can occur. On the other hand, *automation*, as the article goes on to demonstrate, is taken to refer to algorithms but also to a number of other processes equally important to computation, including the relationship instantiated between computers and the wider more-than-human world in which they operate and the imaginaries through which computation is made sense of and understood in situ. At a more granular level still, other work has elaborated on how automation modulates the sensorial capacities enveloped into security practices. A particular emphasis has been placed on the regimes of visibility that automation induces. While a plethora of work has described and assessed the opacity and black-boxed character of automated systems, other work has begun to develop techniques by which such inscrutability might be overcome. Striving more to articulate how vision is inscribed into computational practice itself, Louise Amoore and Volha Piotukh (2015) show that algorithms enact little analytics that render big data meaningful specifically by scything the volume of such data to make patterns perceptible.
2. In some ways, this work echoes that which explores interfaces as an experiential relation between humans, computers and other non-humans (Ash, 2015; O'Grady, 2015).
3. As Elish and boyd (2018: 66) argue, the potential automated technologies bear is central to the imaginary that accompanies them in the here and now, such that 'what technologies can currently do is not as important as what they might yet do in the future'.
4. Balsamo thus writes that 'objects too participate in the designing process by evoking knowledge, stimulating discussion, and manifesting the matter of the world. *In engaging with objects,* human participants create provisional understandings that are communicated in story form' (Balsamo, 2011: 12, emphasis added).
5. Indeed, what for the authors allows the proliferation of such imaginaries in the first place is that they do not address the laborious technical practices that underpin automation.
6. For Ziewitz, this mythology arises owing to the paradoxical character of algorithms as at once all pervasive and ubiquitous but also supposedly inscrutable.

7. In a similar vein, in her book *Designing Culture: The Technological Imaginary at Work*, Anne Balsamo (2011: 5) writes: 'The invention of novel devices, applications, and tools necessarily involves the manifestation of an array of human practices: new languages; new body-based habits; new modes of interactivity; new forms of sociality; new forms of agency; new ways of knowing; new ways of living and dying'.
8. The efficacy such agencies possess has intensified particularly where public authorities suffer from a lack of investment because of austerity politics (Cardullo and Kitchin, 2019).
9. For a thorough examination of agency within and across technologies, see Leese and Hoijtink (2019).
10. Returning to her work on tracing terrorist monies, Marieke de Goede (2012: 87) argues, for example, that 'the risk based approach to financial data mining works to disperse responsibility for security decisions towards and within financial institutions themselves'.
11. The LinkNYC project is said by research participants to have cost CityBridge $300 million thus far. But Dan Doctoroff, chief executive officer of Sidewalk Labs and former deputy mayor of New York, has stated that a lot of capital is being generated for the companies that invested in it (Pinto, 2016). Plotted on some of the most densely populated and expensive streets and avenues in the world, Link kiosk screens offer CityBridge the opportunity to sell to their clients prime advertising real estate using out-of-home marketing strategies informed and targeted according to data that CityBridge has at its disposal. Advertising is the main source of profit from LinkNYC.
12. These criticisms have been voiced by the New York Civil Liberties Union and public advocacy groups such as Rethink Link.
13. Along with emergency communications, LinkNYC supplies millions of denizens and tourists alike with Wi-Fi to which they might not otherwise have access. What is more, CityBridge is obliged to give the New York government $500 million over the project's 12-year duration.
14. Formerly known as the New York City Office for Emergency Management (OEM).
15. Attempts are made to assert that the city itself has sanctioned and bears ownership of the messages projected onto the LinkNYC screens. One interviewee detailed how, on each message, 'we clearly have their logo displayed . . . and we also want to make sure that this message isn't coming from Link, it's coming from the NYC Office of Emergency Management'. The branding on each communication is thus oriented specifically to representing the authority of the city in coordinating the message.
16. These imaginaries evidence a recursive agency here. As Yuk Hui argues, recurrent reiterations of a computational process are never grounded in simple, continuing repetition: 'Recursivity', then, 'is not mere mechanical repetition' but 'is characterised by the looping movement of returning to itself to determine itself while every movement is open to contingency, which determines its singularity' (Hui, 2019: 4). In other words, instead of simply serving as sense-making devices, imaginaries set in motion shifts to practices that have become routine.
17. These abductive forms of reasoning pervade increasingly with the turn to enfolding big data and analytics into security practices. Louise Amoore and Volha Piotukh discuss them when engaging with the industry term *knowledge discovery*, which encapsulates efforts 'to identify previously unknown patterns in a large volume of data' (Amoore and Piotukh, 2015: 351).
18. By incorporating indeterminacy and contingency into the forms of cognition encompassed by it, abductive reasoning, in Parisi's (2019: 27) words, 'argues for the theorization of a sociality of reasoning within the computational strata'.
19. In his discussion of the European Union's Visa Information System, Georgios Gloftsios (2019) also uses the term *ordering* to capture how border technologies play a crucial role in shaping territories.
20. This manoeuvre reflects an argument made by Paul Edwards regarding the routines that develop around the enactment of climate data. For Edwards, the successful establishment of information sharing represents a level of companionship between organizations and a foregoing of any conflict they have. As Edwards (2019: 32) argues, then, 'scientific memory requires truces: acceptance of common standards, suspending conflicts and disagreements to get on with routine data sharing, putting aside political and ideological differences to work together'.

21. As various studies have shown, APIs have developed as a crucial mechanism through which organizations can harvest open-source data to inform a range of enterprises, from advertising to political campaigning.
22. As the authors note, ingestion creates a new situation in which ‘data are no longer strictly collected, but rather are ingested, such that everything becomes available to analysis’ (Amoore and Piotukh, 2015: 345).
23. Enacting forecasts on the back of unclear data is something that Luciana Parisi argues is intrinsic to abductive logics, writing that such a logic ‘engages incomplete information dynamically and thus from within the very process of learning, where abduction works not only to tract data retroactively but also speculatively, by inventing hypotheses that can lead to new rules, axioms, truths’ (Parisi, 2019: 23).
24. Beyond dictating when they should be enacted, these thresholds have been integrated to determine the extent to which LinkNYC kiosks should be mobilized. As the franchise agreement details, during severe or extreme events ‘emergency information . . . will be deployed prominently . . . for at least 50% of the total display time . . . information regarding any imminent threat to public safety will be given a 100% display time until such imminent threat had subsided’ (DoITT, 2014: 2).
25. Indeed, Karine Côté-Boucher has examined how the reshaping of the division of labour brought about by the implementation of new technical practices might be critiqued in relation to the proliferation of discretionary decisionmaking in the case of border security. However, Côté-Boucher (2016: 55) argues that such changes reduced customs officials’ capacity to enact discretion, with technologies adjudged instead to have ‘opened the door to intelligence-led border policing and to forms of regulatory compliance where risk categories are formalized’.
26. Hall demonstrates that discretion is not diametrically opposed to the enactment of legal frameworks. With reference to Georgio Agamben, she argues instead that the manifestation of discretionary powers makes rules clearer. Enacting discretion, according to Hall (2017: 495), involves ‘making sense of rules and making (constrained) choices about their relevance and (non)use in distinct situations’.

References

Amoore L (2013) *The Politics of Possibility: Risk and Security Beyond Probability*. Durham, NC: Duke University Press.

Amoore L (2019) Introduction: Thinking with algorithms – Cognition and computation in the work of N. Katherine Hayles. *Theory, Culture & Society* 36(2): 3–16.

Amoore L and Piotukh V (2015) Life beyond big data: Governing with little analytics. *Economy and Society* 44(3): 341–366.

Amoore L and Piotukh V (eds) (2016) *Algorithmic Life: Calculative Devices in the Age of Big Data*. London: Routledge.

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

Aradau C and Blanke T (2015) The (big) data–security assemblage: Knowledge and critique. *Big Data & Society* 2(2): 1–12.

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

Ash J (2015) *The Interface Envelope: Gaming, Technology, Power*. London: Bloomsbury.

Ayala A and Marvin S (2015) Developing a critical understanding of smart urbanism? *Urban Studies* 52(12): 2105–2116.

Balsamo AM (2011) *Designing Culture: The Technological Imagination at Work*. Durham, NC: Duke University Press.

Barad K (2007) *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning*. Durham, NC: Duke University Press.

Bellanova R and González Fuster G (2019) Composting and computing: On digital security compositions. *European Journal of International Security* 4(3): 345–365.

boyd d and Crawford K (2012) Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society* 15(5): 662–679.

Brayne S (2017) Big data surveillance: The case of policing. *American Sociological Review* 82(5): 977–1008.

Campbell-Verduyn M, Goguen M and Porter T (2017) Big data and algorithmic governance: The case of financial practices. *New Political Economy* 2(2): 219–236.

Cardullo P and Kitchin R (2019) Smart urbanism and smart citizenship: The neoliberal logic of ‘citizen-focused’ smart cities in Europe. *Environment and Planning C: Politics and Space* 37(5): 813–830.

Chandler D (2018) *Ontopolitics in the Anthropocene: An Introduction to Mapping, Sensing and Hacking*. London: Routledge.

Côté-Boucher K (2016) The paradox of discretion: Customs and the changing occupational identity of Canadian border officers. *British Journal of Criminology* 56(1): 49–67.

Crary J (1990) *Techniques of the Observer: On Vision and Modernity in the Nineteenth Century*. Cambridge, MA: MIT Press.

De Goede M (2012) *Speculative Security: The Politics of Pursuing Terrorist Monies*. Minneapolis, MN: University of Minnesota Press.

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

De Goede M, Simon S and Hoijtink M (2014) Performing preemption. *Security Dialogue* 45(5): 411–422.

DoITT (New York City Department of Information Technology and Telecommunications) (2014) Public communications structure franchise agreement: Attachment RDR (resilience and disaster recovery). Available at: https://www1.nyc.gov/assets/doitt/downloads/pdf/Attachment-RDR-Resiliency-and-Disaster-Recovery-(REVISED-FINAL-12-10-2014).pdf (accessed 6 May 2020).

Edwards P (2019) Knowledge infrastructures under siege: Climate data as memory, truce and target. In: Bigo D, Isin E and Ruppert E (eds) *Data Politics: Worlds, Subjects, Rights*. Abingdon: Routledge, 21–43.

Elish MC and boyd d (2018) Situating methods in the magic of big data and AI. *Communication Monographs* 85(1): 57–80.

Evans J (2016) Trials and tribulations: Problematizing the city through/as urban experimentation. *Geography Compass* 10(10): 429–443.

Galloway A (2012) *The Interface Effect*. Cambridge: Polity Press.

Gillespie T (2010) The politics of ‘platforms’. *New Media & Society* 12(3): 347–364.

Gillespie T, Boczkowski P and Foot K (eds) (2014) *Media Technologies: Essays on Communication, Materiality and Society*. Cambridge, MA: MIT Press.

Gloftsios G (2019) Designing digital borders: The Visa Information System. In: Leese M and Hoijtink M (eds) *Technology and Agency in International Relations*. London: Routledge, 164–188.

Graham S and Marvin S (2002) *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition*. London: Routledge.

Hall A (2017) Decisions at the data border: Discretion, discernment and security. *Security Dialogue* 48(6): 488–504.

Hayles NK (2012) *How We Think: Digital Media and Contemporary Technogenesis*. Chicago, IL: University of Chicago Press.

Hayles NK (2017) *Unthought: The Power of the Cognitive Nonconscious*. Chicago, IL: University of Chicago Press.

Hoijtink M (2014) Capitalizing on emergence: The ‘new’ civil security market in Europe. *Security Dialogue* 45(5): 458–475.

Honig B (2009) *Emergency Politics: Paradox, Law, Democracy*. Princeton, NJ: Princeton University Press.

Hui Y (2019) *Recursivity and Contingency*. London: Rowman & Littlefield.

Introna LD (2016) Algorithms, governance, and governmentality: On governing academic writing. *Science, Technology, & Human Values* 41(1): 17–49.

Kitchin R (2014) The real-time city? Big data and smart urbanism. *GeoJournal* 79(1): 1–14.

Lally N (2017) Crowdsourced surveillance and networked data. *Security Dialogue* 48(1): 63–77.

Laurauilt T and Francoli M (2017) Openness, transparency and participation. In: Kitchin R, Laurauilt T and Wilson M (eds) *Understanding Spatial Media*. London: SAGE, 188–204.

Leese M (2014) The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue* 45(5): 494–511.

Leese M (2019) Configuring warfare: Automation, control, agency. In: Leese M and Hoijtink M (eds) *Technology and Agency in International Relations*. London: Routledge, 42–66.

Leese M and Hoijtink M (eds) (2019) *Technology and Agency in International Relations*. London: Routledge.

Lindskov-Jacobsen K and Fast L (2019) Rethinking access: How humanitarian technology control blurs control and care. *Disasters* 43(2): 151–168.

McFarlane C and Söderström O (2017) On alternative smart cities: From a technology-intensive to a knowledge-intensive smart urbanism. *City* 21(3–4): 312–328.

MacKenzie AB (2018) 48 million configurations and counting: Platform numbers and their capitalization. *Journal of Cultural Economy* 11(1): 36–53.

MacKenzie D (2011) How to make money in microseconds. *London Review of Books* 33(10): 16–18.

MacKenzie D (2019) How algorithms interact: Goffman's 'interaction order' in automated trading. *Theory, Culture & Society* 36(2): 39–59.

Marvin S and Luque-Ayala A (2017) Urban operating systems: Diagramming the city. *International Journal of Urban and Regional Research* 41(1): 84–103.

Mattern S (2014) Interfacing urban intelligence. *Places Journal*, April. Available at: https://placesjournal.org/article/interfacing-urban-intelligence (accessed 23 April 2019).

Matzner T (2019) The human is dead – Long live the algorithm! Human–algorithmic ensembles and liberal subjectivity. *Theory, Culture & Society* 36(2): 123–144.

Meijer A and Bolívar MPR (2016) Governing the smart city: A review of the literature on smart urban governance. *International Review of Administrative Sciences* 82(2): 392–408.

Mirowski P (2014) *Never Let a Crisis Go to Waste: How Neoliberalism Survived the Financial Meltdown*. London: Verso.

Monahan T and Palmer NA (2009) The emerging politics of DHS fusion centers. *Security Dialogue* 40(6): 617–636.

Morozov E (2014) *To Save Everything, Click Here: The Folly of Technological Solutionism*. London: Public Affairs.

NYC (2016) Mayor de Blasio announces public launch of LinkNYC program, largest and fastest free municipal Wi-Fi network in the world. 18 February. Available at: https://www1.nyc.gov/office-of-the-mayor/news/184-16/mayor-de-blasio-public-launch-linknyc-program-largest-fastest-free-municipal#/0 (accessed 29 April 2019).

O'Grady N (2015) Data, interface, security: Assembling technologies that govern the future. *Geoforum* 64: 130–137.

O'Grady N (2018) *Governing Future Emergencies: Lived Relations to Risk in the UK Fire and Rescue Service*. London: Palgrave Macmillan.

O'Riordan K (2017) *Unreal Objects: Digital Materialities, Technoscientific Projects and Political Realities*. London: Pluto Press.

Parisi L (2019) Critical computation: Digital automata and general artificial thinking. *Theory, Culture & Society* 36(2): 89–121.

Pinto N (2016) Google is transforming NYC's payphones into a 'personalized propaganda engine'. *Village Voice*, 6 July. Available at: https://www.villagevoice.com/2016/07/06/google-is-transforming-nycs-payphones-into-a-personalized-propaganda-engine/ (accessed 14 May 2020).

Roberts S (2019) Big data, algorithmic governmentality and the regulation of pandemic risk. *European Journal of Risk Regulation* 10(1): 94–115.

Rouvroy A and Berns A (2013) Gouvernementalité algorithmique et perspectives d'émancipation [Algorithmic governmentality and prospects of emancipation]. *Réseaux* 177(1): 163–196.

Silver J (2017) The climate crisis, carbon capital and urbanisation: An urban political ecology of low-carbon restructuring in Mbale. *Environment and Planning A: Economy and Space* 49(7): 1477–1499.

Tanner S and Meyer M (2015) Police work and new 'security devices': A tale from the beat. *Security Dialogue* 46(4): 384–400.

Wajcman J (2019) The digital architecture of time management. *Science, Technology, & Human Values* 44(2): 315–337.

Williams MC (2010) The public, the private and the evolution of security studies. *Security Dialogue* 41(6): 623–630.

Zebrowski C (2019) Emergent emergency response: Speed, event suppression and the chronopolitics of resilience. *Security Dialogue* 50(2): 148–164.

Ziewitz M (2016) Governing algorithms: Myth, mess, and methods. *Science, Technology, & Human Values* 41(1): 3–16.

Interviews cited

All interviews cited in the article were conducted on 24 October 2018.

Nathaniel O'Grady is Lecturer in Human Geography and Disaster in the Humanitarian Conflict Response Institute, University of Manchester. He has published widely on the entanglement of technological innovation within the geopolitics of security.