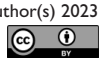
Special issue on *Technopolitics of security*

SECURITY DIALOGUE

Security Dialogue
2023, Vol. 54(1) 76–93



DOI: 10.1177/09670106221139770
journals.sagepub.com/home/sdi


Security technology, urban prototyping, and the politics of failure

Rivke Jaffe
University of Amsterdam, the Netherlands

Francesca Pilo'
Utrecht University, the Netherlands

Abstract

In response to broader political and corporate tendencies towards 'techno-solutionism', critical studies of security technology highlight the threat that security technologies pose to civil rights and democratic accountability. This article argues for a slightly different perspective: rather than taking claims of technological efficacy at face value, it explores the multiple ways in which security-related technology so frequently *fails* to deliver its – confidently anticipated or feared – effects. A focus on sociotechnical failure can offer more comprehensive, on-the-ground understanding of the technopolitics of security. We suggest that these politics may lie precisely in the blurring of concepts of failure and success, as 'prototyping' and experimentation become an increasingly powerful logic of urban governance. This argument is developed through an analysis of security interventions in Jamaica, a context characterized by high levels of violent crime. The article focuses on three technologies that have been adapted to security-related purposes: a communication channel connecting police and private security guards, a public–private CCTV network, and a smart electricity grid. Drawing on approaches from science and technology studies, the article adopts a process-oriented approach, attending to both the discourses surrounding the introduction of these technologies and their everyday interactions with their social and built environments.

Keywords

Failure, Jamaica, prototyping, security technology, technopolitics, urban governance

Introduction

In cities across the world, we see an enthusiasm among municipal governments, police forces, and citizens for introducing new technologies in the fight against crime or the war on terror: from digital sensors and algorithms to the ubiquitous WhatsApp neighborhood groups. It is important to examine this 'technological turn' in urban security and policing critically. While urban security

Corresponding author:
Rivke Jaffe, University of Amsterdam, PO Box 15629, Amsterdam, 1001NC, the Netherlands.
Email: r.k.jaffe@uva.nl

issues tend to be complex social problems, such a turn to technologies offers the illusion of a simple fix that is much easier to implement than long-term social programs. It is always more difficult to reform a police force or to sustain a neighborhood watch than it is to install CCTV cameras or biometric access control. The proponents of such security technologies often present them as neutral, impartial, and cost-efficient, suggesting that they are less prone to error or corruption than security and policing strategies in which human agents play a more visible role. Yet they evidently have their own politics: technology is both produced in specific political contexts and productive of other politics (Winner, 1980).

Recent research in critical security studies has emphasized the role of security technologies in advancing a range of – frequently illiberal – political projects. Digital technologies have come under particular scrutiny. Where governments and corporations promise that algorithms, smart cameras, and other hi-tech innovations are the most effective and efficient way to make nations and cities safer, critical researchers and activists warn that these same technologies enable unprecedented forms of surveillance and control, while their proprietary nature inhibits democratic oversight (see, for example, Ferguson, 2016). We largely concur with such critiques and hold that close academic and activist scrutiny of the technopolitics of security is essential. In this article, however, we propose a shift in analytical focus, towards the many ways in which security technologies – especially when they are actually implemented – fail to live up to both their promise and their threat.

In this article, then, we focus on the politics of technological failure. Drawing on approaches from science and technology studies, we explore these politics through a process-oriented approach that attends to the everyday interactions between technologies and their social and built environments. Such an engagement with the social life of technology over a longer period of time can highlight how and why technologies fail to live up to their alleged potential, to achieve their stated goals. It also pushes us to reflect on what political outcomes sociotechnical 'failure' enables. Our analysis suggests that these outcomes may involve the blurring of concepts of failure and success, as 'prototyping' and experimentation – rather than, for instance, accountability – become an increasingly powerful logic of urban governance. Drawing on a combination of media analysis and ethnographic research in urban Jamaica, we analyze the promotion and/or introduction of three distinct technological devices:[1] a communication channel connecting police and private security, a public–private CCTV network, and a smart electricity grid. While all these cases represent technology-focused security interventions, they reflect a diverse range of technologies, governance actors, and publics. In all three instances, technology is promoted as enabling an efficient response to the multiple challenges that urban governance actors face in addressing security issues, from public and private actors for whom security is their core business, to a private electricity provider facing the combined challenges of urban violence and financial losses. This inclusion of governance actors beyond the state – reflecting ongoing processes of security privatization and pluralization[2] – enables an analysis of the various interests that technological interventions may serve within the broader urban security landscape.

Our analysis emphasizes the politics of the narratives that emerged around the introduction of each device, highlighting the performances and contestations of sovereignty at stake in such narratives. Beyond a discursive analysis, we seek to complicate such narratives by tracing the fate of these technologies over time and in practice. For each device, drawing on interviews, observations, and media reports,[3] we explore how and why it failed to deliver on its initial promise, and seek to unpack the politics of these failures by asking which new political or economic pathways – or successes – are enabled by apparent failures.

We start the article with a reflection on the tendency towards alarmist narratives within critical studies of security technology and outline a sociotechnical approach that focuses on technological

failures and their politics. Next, a background section presents a brief outline of security governance challenges and the turn to technology in urban Jamaica. This is followed by an analysis of the three security-related technologies. We conclude by connecting this analysis to a discussion of the ways in which failure has been reconceptualized in urban governance.

A sociotechnical approach to urban security politics

Critical studies of security technology have tended to be dominated by political science and international relations research, focusing on national security, border regimes, and anti-terrorist measures. Within this field of study, much attention has gone out to hi-tech digital surveillance, a multi-sensory panopticon that combines military and corporate logics to track our every move while reinforcing discriminatory logics (Bigo, 2006; Muller, 2010; Shaw, 2016). As this security technology also creeps into urban policing and smart city strategies, we see critical urban studies expressing a related concern, focused more specifically on the militarization of cities and discriminatory urban policing (see, for example, Graham, 2011; see also Ferguson, 2019).

Academic and activist engagements with security technology have presented strong critiques of what Evgeny Morozov terms 'techno-solutionism'. Discussing the recent embrace of 'big data' and the digital quantification of behavior as the solution to a broad range of social problems, Morozov (2013: 5) describes how 'complex social situations [are recast] either as neatly defined problems with definite, computable solutions or as transparent and self-evident processes that can be easily optimized – if only the right algorithms are in place!' He calls this optimism 'technological solutionism', arguing that digital technology presents highly efficient but dehumanizing solutions for phenomena that are either not a problem at all or much too complex for an easy fix. He also points to the shift in power that results when digital technology is pitched as the solution to everything: technology companies, rather than elected governments, will shape the future of our cities and societies.

While these critiques are urgent, they can sometimes slide into alarmist narratives, which have multiple limitations. First, an overly dystopian view of security technology can be politically problematic: By suggesting that security technologies live up to their claims of efficiency and effectiveness, such narratives risk empowering the corporations and politicians that promote them. When alarmism slides into fatalism, it also risks disempowering the citizens who interact with these technologies, paralyzing us rather than spurring us to action. Representing digital technologies as all-encompassing or terrifyingly successful in their efficacy, then, runs the risk of amplifying the techno-solutionism of corporations and governments. Second, totalizing narratives of technological doom – whether attributed to the surveillance state or robot overlords – are frequently too universalist and imprecise to help us identify effective action. Such narratives are not always based on in-depth empirical analyses of technologies following their actual implementation and everyday use. In fact, many studies of security technologies that are actually in place in the real world find that the technological devices involved do not live up to their promise at all (e.g. Adelman, 2018; Andersson, 2016; Magnet, 2011). It is tempting to conclude that many technologies of urban policing and security are complete failures.

Conceptually speaking, both technological solutionism and its critical counterparts risk invoking a technological determinism that overemphasizes the role of security technology in shaping society, without necessarily developing detailed empirical accounts of what technologies actually end up doing (or not doing) in practice.[4] We suggest that making academic knowledge of technology actionable requires more precise accounts of how technology is utilized, appropriated, and adapted in specific contexts. Such accounts are well served by a sociotechnical approach: drawing on insights from science and technology studies scholars such as Wiebe Bijker, Stephen Woolgar,

and Bruno Latour, such an approach understands the political effects of technologies as emerging in non-linear ways from dynamic and contingent relations between humans and non-human entities. While such a sociotechnical approach is increasingly applied to the development and implementation of security technologies, not least in this journal (see, for example, Bellanova et al., 2020; Bourne et al., 2015; Jeandesboz, 2016), overall, authors working in this tradition have spent less time unpacking the political and economic logics of failure and success as they emerge in practice.

Our interest here is not so much to distinguish between 'good'/successful and 'bad'/failed technology, but to understand what strategic work failure does, for whom, and how. Rather than understanding failure as a condition that can be identified objectively, we approach it as a contingent outcome of ongoing, contested processes of valuation. Technologies possess 'interpretative flexibility' (Pinch and Bijker, 1984: 409): the meaning of an artefact is unstable and varies across its relations with different social actors, extending far beyond the intentions of its designers.[5] For example, a security technology that its engineers consider a success in terms of the learning it enables may well end up being viewed as a total failure by the security officers who use it in practice (Lisle, 2018: 893). Accordingly, we understand technological failure and success not so much as objectively identifiable, polarized states, but as sociotechnical constructs that not only derive from the position of evaluators but also often serve to legitimize their situated interests. The labels of 'failure' and 'success' can function as core elements within larger political narratives and performances (see Fincham, 2002: 7).[6] Indeed, in line with the focus of this special issue on technopolitics – that is, in scrutinizing 'the ability of competing [security] actors to envision and enact political goals through the support of technical artefacts' (Gagliardone, 2014: 3) – we seek to interrogate the political work that the sociotechnical constructs of failure and success do in the world.

The technopolitics of failure and the logic of urban prototyping

In our analysis of the technopolitics of urban security and policing, then, we propose avoiding technological determinism by dwelling a little longer on the various *failures* of urban security technology. We are interested in discussing, first, what is understood as failing and why it is seen as such. In so doing, we also take note of Peter Adey and Ben Anderson's (2012: 113) call to pay more attention to how 'apparatuses of security fall apart, fail, are disrupted, or are held together', while placing our emphasis on the role of specific technological devices within such wider apparatuses. There are various ways in which security technologies can fail, which emerge from the inevitable interaction of those technologies with their social and material surroundings: there are failures related to subversion, hacking or dual use; those caused by people's capacity to bypass or circumvent the technology; but also failures related to less intentional, more mundane types of social or material breakdown connected to off-script uses and disrepair. Getting security technologies to 'work' requires various type of labor (Vukov and Sheller, 2013; see also Graham and Thrift, 2007): the labor of various security and technology professionals, from software designers to police officers and security guards and their supervisors. It often also involves the labor of those being policed or 'secured'; if they actively circumvent or subvert the technology, it is also less likely to work.

Specifically, though, in thinking about how and why different types of failure emerge, we concentrate on the *politics* of technological failure. Just noting that a security technology has failed in practice is evidently not enough – we have to ask for whom it failed, for whom it might still have been a success, and what new political or economic possibilities it may have established. We are interested in scrutinizing the political dimension of what Debbie Lisle (2018: 891) calls the agency of failure, tracing 'the work that [failure] does in the world to guide practice, change behaviour, recalibrate relations, alter materialities and mobilize futures'. As our analysis of Jamaica's urban

security landscape shows, some of the futures made newly possible through technological failure involve easily recognizable political and economic benefits to individuals or organizations. In addition, however, in the process from idea to design to (non-)implementation to reconceptualization, the various technologies we discuss in this article also work as de facto (rather than formal) 'prototypes' for how to govern urban spaces and populations.

The logic of prototyping, which has become increasingly popular in urban governance, blurs longstanding understandings of failure and success. As Alberto Corsín Jiménez (2014: 381) notes, 'An important feature of prototyping . . . is the incorporation of failure as a legitimate and very often empirical realisation.' Within urban governance, failure is increasingly anticipated as a natural outcome of experimentation, while 'design thinking' replaces older logics of planning. New technologies, we suggest, may act less as 'solutions' or 'fixes', and more as experimental forms that facilitate learning by doing, a process in which trial-and-error is taken for granted rather than necessarily viewed as a waste of money or cause for political scandal.[7] However, this sociotechnical process should be scrutinized carefully in terms of the political relations it establishes or consolidates. As Martin Tironi (2019: 504) suggests in his analysis of urban prototyping as a political device, 'One distinctive element of the experiments undertaken by civic authorities and urban agencies is that the design, dramaturgy and *mise en scène* of these interventions are just as important as the results of the experience or even more so.' Analyzing these interventions as performances involves taking the materiality of the security technologies seriously, while also attending to the political narratives – of problems and solutions, authority and responsibility, success and failure – that surround them as they enter and exit the stage of urban security governance.

Below, drawing on our research in urban Jamaica, we discuss a number of technological failures in urban security and policing interventions. To provide the context needed to understand the political work that various 'failed' security technologies do, we first provide a brief background to urban security governance and the technological turn in Jamaica.

Security governance and technology in urban Jamaica

Jamaica suffers high levels of crime and violence, connected to a history of political turmoil, high levels of inequality, and other social factors. Homicide rates increased sharply in the second half of the 20th century, climbing from 17.6 homicides per 100,000 population in 1976 to 43 in 2001 (Harriott, 2003: 7). Over the past two decades, this rate appears to have stabilized somewhat, hovering around 47 per 100,000 in 2019, still three times higher than the average for Latin America and the Caribbean.[8] Jamaica's public security structure faces multiple challenges, with many citizens viewing formal institutions, and especially the police force, as ineffective, abusive, and corrupt. This has contributed to a crisis of public safety, manifest not only in the high levels of violence and the ineffective response of public institutions, but also in the rise of multiple security providers. In addition to the state's deployment of both the Jamaica Constabulary Force (JCF) and the Jamaica Defence Force (JDF) in urban policing, residents have turned to a growing number of formal and informal non-state security actors.

The capital of Kingston, where much of the violent crime is concentrated, with a homicide rate of 169 per 100,000 population in 2018,[9] represents an especially heterogeneous landscape of security governance. Corporate actors and residents of wealthier neighborhoods in uptown Kingston tend to turn to private security companies for protection, relying on high walls, electronic alarm systems, and armed-response guards for security. In contrast, in low-income neighborhoods in downtown Kingston, so-called dons – community leaders often involved in criminal activities – are often central to more informal systems of non-state security provision (Campbell, 2020). Over several decades, these dons have increasingly assumed an informal governance role in what are

known as garrison communities, 'geographically discrete, fortressed urban areas marked by poverty, gang violence, political manipulation and confrontational relationships with law enforcement institutions' (Mullings, 2019: 141). In these areas, residents often have no choice but to turn to criminal organizations for security.

Within this fragmented security governance landscape, the most emblematic and mediatized attempt of the state to (re-)establish a primary role in security governance was the 2010 'Tivoli Incursion'. This security operation, during which the Jamaican military and police killed 69 citizens, concentrated on the garrison community of Tivoli Gardens and was aimed at capturing and extraditing Christopher 'Dudus' Coke, the country's most powerful don. The 2010 security operation was accompanied by a state of emergency in sections of the country that lasted more than a year, during which curfews and other 'anti-gang' measures were implemented in low-income areas. These forms of exceptional policing – resembling urban 'pacification' efforts in Rio de Janeiro and other cities – were expanded in subsequent years. In 2018, the Jamaican government established new states of emergency in the most urbanized parts of the island and introduced Zones of Special Operations (ZOSOs), special security zones where curfews enforced by joint military–police operations were to be combined with community development efforts.

In combatting crime, state and commercial security actors have frequently highlighted the potential of incorporating new technologies (including new forms of digital surveillance) in enhancing their capacity to detect, deter, apprehend, or prosecute criminals and to work together effectively across public–private divides. This is the case both in low-income neighborhoods and in wealthier urban areas. The Ministry of National Security's recent *Five-Pillar Strategy for Crime Prevention and Citizen Security* places particular importance on the acquisition and use of technology, asserting that 'in engineering a seamless, effective, all-of-Government anti-crime machine, few factors are as important as the procurement, and full deployment, of appropriate technologies' (Ministry of National Security, 2017: 106). More recently, the commissioner of police, Major General Antony Anderson, proclaimed that the JCF was 'in the midst of an aggressive technology-based drive to create a modern, connected and highly efficient police force' (Smith, 2020). In a parallel move, private security companies have also been expanding the range of technologies they offer to clients, from CCTV surveillance and smart home systems to biometric access control and GPS-based vehicle trackers (see, for example, McKinson 2017).

What technopolitics can we discern in the narratives surrounding specific technological devices? To what extent do these various technological devices achieve their stated goals, and what politics are at work when these security interventions end in sociotechnical failure? Below, we address these questions in an analysis of three distinct devices. First, we discuss attempts to introduce a radio communication channel connecting Jamaica's private security guards to the police.[10] This analogue communication technology was supposed to act as what is sometimes called a 'force multiplier', extending the reach of the JCF's eyes and ears to the many sites surveilled by private security guards. In addition, the communication channel was supposed to improve private security access to the JCF, enhancing guards' ability to respond to suspicious activities. However, a pervasive social taboo on 'informing' – sharing information on criminal activities with the police – meant that this technological alignment of guards with the police presented a serious threat to the lives of the guards.

The second case, the JamaicaEye public–private CCTV network, was a follow-up to these attempts. Again, a technical fix was proposed to enhance 'interoperability' between public and private security systems, expanding surveillance while also supporting criminal prosecutions by providing a visual form of legal evidence in the absence of witness testimonies. This time, however, the technology sought to connect security cameras operated by the police and military to

those owned by private citizens. While the system is still being expanded, early reports suggest that technical breakdowns and a lack of police follow-up are severely hampering JamaicaEye's impact.

The third device we analyze is that of the smart grid developed by Jamaica's electricity utility, the Jamaica Public Service Company Limited (JPS).[11] Following the 2010 Tivoli Incursion, the JPS intensified its efforts to 'regularize' electricity consumption in low-income, high-crime neighborhoods (so-called 'red zones'),[12] where electricity theft is high and JPS staff face the risk of aggression when checking meters or disconnecting illegal 'throw-ups'. In this context, smart metering – by enabling the JPS to monitor and control its infrastructure at a distance – functions as a security technology: it is seen as capable of protecting company revenue, infrastructure, and staff. However, communication signal failures and continued on-site tampering mean that the smart grid has had little long-lasting impact on electricity theft.

From technological fix to failure

We analyze the social life of these three technologies over time by tracing three phases. First, we discuss the narratives that presented each technology as a fix to a specific security challenge: we ask how security-related problems were framed to match a technological fix, while exploring which political claims and economic interests this techno-solutionism served. Next, we unpack the social and technical aspects underlying the failure of each technological fix in practice. Finally, we explore the politics of these failures, suggesting the ways in which each failure might still signal a form of success, albeit not in terms of the originally stated objectives, and how this connects to an emergent logic of prototyping in urban security governance.

Promoting a technological fix: Framing problems and solutions

In each of our three cases, governance actors constructed a problem narrative that proposed a specific technological solution to security problems, with both problem and solution connected to political claims. In the first case, this narrative put forward a shared communication channel as the technological fix for the problem of uncoordinated public and private security efforts. In Kingston, the number of private security guards is about twice that of JCF officers. Although formally these guards are responsible only for the safety of a specific property or the people within it, they frequently witness crimes or security threats in public space. At multiple points in time, Jamaica's Ministry of National Security sought to tap into these eyes and ears on the street. One important attempt involved the use of a dedicated radio communications channel, repurposing an existing type of technology as an anti-crime tool by connecting security guards to the JCF. This channel would allow guards who witnessed anything while on duty to access the police directly through their own radios, without going through the notoriously dysfunctional emergency telephone number 119. The idea was that the radios would seamlessly connect the thousands of security guards dispersed throughout Kingston to the JCF, translating their observations into actionable police information.

The problem, then, was constructed as a lack of communication and coordination between public and private security actors. In this framing, the pluralization of policing was not indicative of institutional failure. Rather, Kingston's fragmented landscape of security provision was presented as an opportunity: it could be transformed – through enhanced communication technology – into a collaborative effort to tackle crime and violence. This vision has been central to successive security policies, which have underlined the need for public–private partnerships, connecting state security actors to private security companies but also heavily stressing citizen participation in policing. Such a narrative centered on the need for partnerships allows the police and military to perform

claims to state sovereignty, coordinating rather than monopolizing security provision while shifting responsibility across a broader network of actors.

The second case, which can be understood as something of a follow-up to the first, involves a comparable promotion of technological integration of state and non-state security efforts. Here, the state security forces proposed the integration of private CCTV feeds – from cameras facing public spaces – into a networked system called JamaicaEye, with the police monitoring the video feeds but the military overseeing the central network. Again, this narrative promoted the idea that technologically mediated information-sharing would herald a major improvement in crime-fighting. In JamaicaEye, however, the security-related problem was framed less as a disconnect between commercial and state security providers and more as the need for citizens to be active participants in crime prevention programs and security provision. As the project's website proclaimed, 'Jamaica, YOU can help. Connect your camera system to the JamaicaEye national CCTV network and help to make Jamaica safer.'[13]

Successive national security policies and public campaigns have placed a major emphasis on citizen participation. An early iteration is found in the 2007 National Security Policy, which states that 'there needs to be a radical change in the way in which everyone views his or her responsibilities for national and community safety and security. There needs to be the recognition that "security is everybody's business", and not the sole responsibility of the police and other law enforcement agencies' (Ministry of National Security, 2007: 38). A follow-up policy similarly stressed this responsibility: 'In keeping with the initiative to develop a stronger partnership between citizens, civil society and all Government organizations involved in delivering security services, it is important for all members of the public to understand the critical role that they are required to play in helping to make Jamaica a more safe and secure place to live and visit' (Ministry of National Security, 2013: 93). This narrative reflects a broader global tendency towards neoliberal responsibilization in security governance. Where this responsibilization has often focused on the importance of citizens sharing information with the police and testifying against criminals in court, JamaicaEye provides a technological solution to a widespread unwillingness to do so by removing humans from the equation. Calling the cameras a 'force multiplier', Minister of National Security Horace Chang announced: 'It will have the requisite monitoring systems to collect and store high-quality footage that can be used as evidence in our courts. . . . This investment in JamaicaEye will give the police the appropriate counter-strategy to intercept and curtail the movements of criminal gang members, the dons and their facilitators.'[14] The CCTV network draws on citizens' resources to provide the police and courts with evidence of crimes, but shields private citizens from the risks involved in this process of informing and testifying.

In the third case, the problem–solution narrative was framed by the JPS, a public–private utility company rather than a government agency. Here, the problem was commercial and security risks, the two seen as intertwined in low-income, high-crime 'red zones' (Interview 1). The commercial risk involved high rates of 'non-technical losses', that is, electricity theft: some 18% of the net generation in 2018, but over 70% in most of these zones (JPS, 2019). A JPS official stated that when its agents attempt to cut off illegal connections, they face significant aggression and are often unable to visit these areas without police accompaniment (Interview 2). In addition to residents protesting disconnection, dons and other criminal actors play an important role in deterring JPS from its attempts to reduce theft. The technological fix for this commercial-security challenge was the smart grid, in the form of the 'Residential Automated Metering Infrastructure' (RAMI). The security governance aspect of electricity management was exemplified by the first installation of the smart metering in Tivoli Gardens, after the 2010 security operation (Radio Jamaica News, 2011). The reassertion of state sovereignty through this operation and the intensified

policing strategies that followed offered the company an opportunity to regularize electricity access, dismantling illegal connections and registering customers.[15] Since 2010, JPS has used the RAMI system in 'red zones' as a technical instrument to regularize illegal connections. Not only did the presence of the state security forces and the initial destabilization of the dons' governance following Dudus's extradition reduce the security risks of JPS's attempts to recover commercial losses, but the installation of the RAMI system was also seen as a preventive technology to manage current and future security *and* commercial risks.[16]

The RAMI system – which involves integrated digital meters, data management systems, and two-way communication networks – enables important changes in the management of JPS's relations with its customers. Its features allow JPS to remotely execute a number of important operations that previously required a physical presence, such as measuring electricity consumption levels, connecting and disconnecting customers, detecting tampering, and more accurately identifying variations in individual consumption that indicate electricity fraud. This automation of the different operations minimizes the human interaction between customers and (often subcontracted) technicians and electricians that JPS associates with both corruption[17] and potentially violent conflicts surrounding disconnections. The RAMI system also features an anti-theft design, with meters installed in locked cabinets located on electric poles rather than in customers' homes, and medium-voltage distribution lines replacing low-voltage (secondary) lines to discourage tampering by increasing the risk of electrocution (see Figure 1). Alarm systems that detect cabinet tampering shut down all meters in one cabinet, a punitive measure aimed at encouraging horizontal control between customers. These combined features were all aimed at replacing or mediating human interventions and contact with automated technology.

Sociotechnical failure in practice

These three technological fixes each failed in their own way. The first instance, involving communication technology, failed to recognize the charged sociopolitical environment in which security-related communication takes place. The implementation of the radio frequency supposed to connect public and private security professionals was planned by the Ministry of National Security together with the Jamaica Society for Industrial Security (JSIS), the commercial security sectoral organization. However, during this planning phase, a new minister took over the national security portfolio. In his enthusiasm, and perhaps in an attempt to generate positive publicity, he went on national TV and radio to announce the development of the shared public–private security communications channel, where the security guards would inform the ministry or the police of any crimes they witnessed. The minister suggested that security guards could also report on crimes witnessed outside of their workplaces given that they tend to live in so-called volatile areas.

However, this immediately caused major problems for guards. As one private security company manager explained: 'The security guards couldn't go home, because the people in the community know' (Interview 3). This mention of 'people in the community' was a reference to the fact that many security guards live in low-income urban areas where criminal organizations have a strong presence. In these neighborhoods, where dons enforce the rule that *informer fi dead* (informers must die), talking to the police can mean running the risk of being killed. The proposed use of a public–private radio channel – a useful technology allowing the police to access information that would otherwise elude them – ended up posing a threat to the lives of security guards whose low-pay, high-risk jobs already placed them in a vulnerable position. To protect their labor force, the private security industry group JSIS had to formally deny that they were engaged in any such partnership with the JCF. As the manager explained,

Figure 1. The RAMI system (photograph by Francesca Pilo').

> In Jamaica you have to be very, very careful. Because we will jeopardize the lives of the security guards and even something can happen, you know, in the community, and the police respond to it, and the guard who lives there has nothing to do with it and they will kill him and his family. (Interview 3)

In other contexts, a shared radio frequency connecting private security guards and the police would not necessarily lead to such controversy. However, the *informer fi dead* rule that is prevalent in and beyond Jamaica's inner-city neighborhoods politicizes this communication technology to the extent that it could be a lethal object. The state security forces framed the adaption of communication technologies into tools of policing and surveillance as an opportunity to harness the eyes on the streets to bolster the police's reach. Yet the initiative ran aground on the same features of those streets that it was meant to control.

The second instance, the public–private CCTV network JamaicaEye, is still operative, but has arguably also already failed. Launched in March 2018, the project involved plans to expand from 500 state-owned cameras in high-priority areas to 1000 in the short-term, matched by community-based initiatives to procure, install, and connect privately owned camera systems, moving towards the end goal of a total of 5000 connected cameras across the island. However, various cybersecurity issues emerged in the design and rollout of the JamaicaEye infrastructure. The CCTV network's

'secure' system of information-sharing and communication proved physically compromised. Because of ongoing roadwork in Kingston, the secure physical fiber-optic cables that were supposed to guarantee cybersecurity were inoperative, and JamaicaEye had to rely on cables managed by external parties. More worryingly perhaps, the connection of private cameras to the system was based on criteria related to image quality, but there were no cybersecurity requirements; given the system's dependency on these private connections, this meant that the system as a whole could potentially be compromised at any time (Svensson and Rydén, 2019: 43).

In addition, within a year it appeared that many of the first set of state cameras had already broken down and gone unrepaired, as critical voices began to ask 'how many of these cameras work, whether they are really being monitored, and if they are delivering value to taxpayers' (*Jamaica Gleaner*, 2019). Two years into the project, the only public 'success' attributed to JamaicaEye was the identification and apprehension of the owner of a taxi that had mowed down a police officer. This caused observers, such as one letter writer, to ask: 'Where has Jamaica Eye been all this time . . . ? Wasn't this network of surveillance able to pick up robberies taking place? . . . I haven't heard any reports of its effectiveness until the tragic incident involving the lawman' (*Jamaica Gleaner*, 2020). The network of eyes appeared not to be seeing many incidents with potential for criminal prosecution, and after a few years the JCF social media promotion of the system had shifted towards emphasizing its role in traffic management over crime control.

In the case of the RAMI smart grid, the core issue that affected its rollout in 2018–2019 was the faulty communication network between JPS and its 'red-zone' customers. This communication failure meant that JPS could not accurately measure customers' monthly consumption through remote access, and that disconnection and reconnection operations were not undertaken at that time (Interview 4). Different JPS employees listed multiple reasons for the system's communication dysfunction. A JPS engineer, for example, explained that the initial technology adopted at that time, the power line carrier (PLC) communication system, was not working correctly because of conflicting radio frequencies (Interview 4). Accordingly, JPS sought to replace the PLC-based Quadlogic system with one considered to have a more solid communication platform.[18] But the communication system's malfunction was also attributed to corruption. It was reported that the communication system failed because customers had already found a way to hijack the system, either on their own or with the help of JPS agents, and this tampering often damaged the communication modules. As one JPS manager explained:

> With the RAMI system, if they try to breach the system, it can result in the communication model being burned or the meter itself being burned. We have a lot of modules burnt because still you have persons who are stealing, and it interferes with the communication. (Interview 6)

It is difficult to distinguish 'human' from 'technical' failures here, as the communication system's failure emerged from the technology's interaction with the actually existing urban environment in which it must operate. The technology itself generates conflicts surrounding electricity payment, as it transforms the ways in which JPS and its customers interact with each other and with the physical infrastructure. Together, the physical tamper-prevention measures and the remote communication system changed these interactions, but these devices did not fulfill their promise as the technological solution to theft and aggression against agents.

The politics of failure

How might we understand these various sociotechnical failures, the inability of these technological fixes to address Jamaica's problems of crime and insecurity? Some might suggest that these

failures are due to bad luck, human fallibility, or technology transfers 'inappropriate' to the Jamaican context. Indeed, we can recognize a political dimension in where the blame for the failure of security technologies is directed. Sometimes uncooperative or unskilled humans are blamed; at other points, failure is 'displaced out of the human realm and onto the device itself' (Lisle, 2018: 893). But to only emphasize this might be to miss something important about the politics of technological failure. Rather than pursuing explanations along these lines, we approach these failures as productive, as agentively generating new political or economic pathways that should be explored, as well as suggesting a new logic of urban security governance. Even if each technology does not work in the way its proponents originally claimed it would, within the dynamic process of technology-in-practice, it makes other things happen (compare Mosse, 2005).

A new technology may enable new economic redistributions to take place, make political commitments visible, strengthen relationships, or allow new understandings of the original problem to emerge. In a broad sense, even the most dramatic failures can still involve success for key individuals or organizations. This might involve corporate profit, with politicians and bureaucrats getting a cut, or the failure could at least bolster the career of those same political actors by proving their readiness to act, their capacity to be bold and creative. Security studies has stressed this performative role of technology; as Didier Bigo (2006: 55) notes, 'the large-scale mobilization of money and technology is supposed to convince the people that the government cares about their safety and is doing what needs to be done'.

This performative dimension was at least partly at work in the context of the radio channel connecting police and private security guards, but the minister's eagerness to claim the technological fix immediately provoked the threats against guards that made its implementation a non-starter. Yet it is possible that this early failure provided important lessons for senior managers in the public and private sector, highlighting the need to more actively consider the volatile context of donmanship in which any technological intervention would be rolled out. In the years that followed this initial attempt, quieter, less technology-based attempts at information-sharing were developed. In 2016, for instance, a memorandum of understanding was signed between the 'JCF and [private security sectoral organization] Jamaica Society for Industrial Security (JSIS) to facilitate the strengthening of mechanisms for vetting, facilitate cooperation for the sharing of information where authorised, and execute industry-specific training to bolster the capacity of the private security industry' (Ministry of National Security, 2017: 112). Unlike the early 2000s memorandum of understanding, this initiative was not visible in the media.

The JamaicaEye camera network did more important work in enabling political performances, showing a political willingness to tackle crime in innovative ways, while recognizing the problems posed by the *informer fi dead* rule that blocked the public–private radio channel. It worked as visible evidence that 'something was being done' by the government to address the impunity of criminals, while also providing material-technological support for the policy emphasis on citizen participation in crime-fighting. However, here explanations might be found more directly in the economic realm. As some critical voices suggested,[19] security budgets present a lucrative proposition to technology suppliers and developers, who may invest significant energy and funds in lobbying politicians for, and generating media interest in, a specific technological fix. These economic interests are evident to some Jamaican citizens, who immediately suspected corrupt deals between business and political elites. Many others, however, received the same technological initiatives enthusiastically, and remain enthusiastic about them, despite a lack of examples of JamaicaEye's providing crucial evidence in any court cases five years after its initial roll-out.

The politics of the smart metering failure were productive in related but distinct ways. Conceived as an instrument to improve the corporate management of territories through the

remote monitoring and policing of resident behavior, the communication system's failure to live up to this potential had other political effects. First, it has contributed to the emergence of a new approach to electricity theft in 'red zones', feeding into JPS's development of a 'more holistic' approach to the reduction of non-technical losses through a community renewal program.[20] As the manager of JPS's community program explained, 'We have tried with the RAMI solution, but we realized that just putting a technical solution alone *will not survive*. So, we decided to create a community renewal program' (Interview 1, emphasis added). The statement that 'a technical solution alone will not survive' not only acknowledges that this technology failed to deliver, but also recognizes the limits of any technological fix to such a complex problem. It also suggested a recognition of the co-evolution between technology and human action (including corruption), at least for the time being. One engineer explained the RAMI system's failure by stating that the technology was still 'not mature' – meaning still too vulnerable to human corruption – and suggesting that in the future a more efficient technology might be designed (Interview 4). Even if the RAMI system is no longer considered *the* technological fix for fraud, it is still presented as a complementary and important solution.

The political implications for the provider–customer relationship are also emerging. Initially, JPS stressed the RAMI system's importance in tackling theft and (in)security in the media, describing the technology as a 'weapon to fight against non-technical losses' (Dutta, 2009). This public emphasis on the potential of this technological solution in addressing electricity theft can be understood within the regulatory context. The JPS recoups part of its theft-related losses from paying customers by increasing electricity tariffs, but has a regulatory obligation to adopt concrete measures to reduce such losses and thereby minimize tariff increases. The idea of a technological solution, then, was an important element within a political performance aimed at crafting an image of a provider that recognizes the interests of all its (paying) customers. More recently, politicians have begun to question the RAMI system's reliability and presented the dysfunctional communication system technology as violating customers' rights, given that it resulted in customers receiving bills based on estimated rather than actual use for months on end (Frater, 2019). Just as the potential functioning of this system invited attention to how it could reshape power relations, so its failure invites a similar perspective.

As these examples show, failure is rarely the end of a sociotechnical process: the social life of a security device – from its conception and design to its (non-)implementation and reconceptualization – enables political and economic outcomes that were less feasible previously. In addition to generating short-term political and economic benefits to politicians, businesses, or government agencies, the technologies we have discussed here can also be understood as 'prototyping' forms of urban security governance. As Martin Tironi (2019: 515) explains, the function of a prototype 'cannot be reduced to a simple evaluation of a preconceived idea'. He distinguishes between problem-validating prototypes, which can be understood as sociomaterial inscriptions of a specific vision, and problem-making prototypes, which generate 'situations of uncertainty and frictions that produce opportunities for transformation and redefinition' (Tironi, 2019: 516). Our Jamaican examples are a mix of both: the communication channel and JamaicaEye were inscriptions of a security governance vision in which private security companies and citizens assume a responsibility for security alongside the police and military, normalizing this form of pluralized security governance.[21] The 'red zone' frictions that thwarted the communication channel and the smart grid, however, also generated important insights into the stubborn nature of the sociopolitical context of urban Jamaica, in which problems and potential solutions came to be at least partially redefined. In short, these were not failures, but learning opportunities.

Conclusion

Many governments, companies, and citizens are disappointed by the ability of public and private security forces to act effectively. Often, human fallibility – inattention, lack of training, corruption – is seen as the cause for this lack of effectiveness. The assumption that technology eliminates this human element underlies the optimistic turn to quick-fix solutions, with hopes and dreams of safer cities projected on a range of hi-tech and low-tech devices. This optimistic 'techno-solutionism' relies on an understanding of technology as neutral, a perspective that is increasingly debunked by more critical accounts, which signal the various threats these technologies entail to social and political rights. In this article, we have proposed a slightly different approach to the politics of technology, by focusing on technological failure and adopting a sociotechnical approach that follows a technology from design to roll-out and (non-)implementation, including its everyday interactions with the urban environments, in order to understand its on-the-ground political effects.

In pursuing such an approach, we take seriously Peter Adey and Ben Anderson's (2012: 100) call to understand 'the workings of security apparatuses beyond an exclusive concern with the logics that animate [security] and their apparent success'. Here, we have sought to underline the political work of specific technical elements within such apparatuses, considering their failure in relation to their original animating logics, but still seeking to identify a broader rationality of governance at work – that of prototyping. In a world of experimentation, technological failure has become a mundane event rather than a political problem, much less a spectacle. Failure has come to be seen as productive, and boundaries between failure and success have become blurred within political discourse. Public policymaking in cities increasingly relies on prototyping – a logic previously associated with design – in developing a model of urban governance characterized by flexibility, provisionality, and anticipation. Urban governance, including security governance, involves prefigurative experiments focused on technological innovations and adaptations, which institutional actors – whether the police or a commercial organization – hope will generate a new and improved city of the future, even as they anticipate their failure. Rather than being conceived in terms of delivering measurable outcomes or meeting preset targets, the 'success' of technologies or policies may be reframed in terms of increased learning opportunities or the habituation and support of various constituencies. In short, to evaluate the success of security technologies in terms of the results proponents originally claimed they would deliver may be to miss one of the main points of prototyping. Concrete, quantifiable results are less important than *attempts* to inscribe specific ways of administering urban life. Analyzing 'failing' technologies through the lens of prototyping enables an understanding of technopolitics that goes beyond current approaches, while forming a useful counterbalance to studies that highlight other types of technologically assisted anticipatory politics.

Acknowledgements

We are grateful to Frank Müller and Matthew Richmond for their editorial support in developing this article as part of their special issue on technopolitics.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The article draws on research funded by the European Research Council (grant agreement no. 337974, SECURCIT) and the Netherlands Organisation for Scientific Research (grant no. 452-12-013). In addition, it draws on postdoctoral fellowships funded by the University of Amsterdam's Centre for Urban Studies (CUS) and the Belgian Fonds de la Recherche Scientifique (FNRS).

ORCID iD

Rivke Jaffe https://orcid.org/0000-0002-6115-2978

Notes

1. Following Amicelle et al. (2015: 294), we use the term 'device' here to refer to 'an artefact, a piece of equipment or an instrument made or adapted for a particular purpose, as well as a plan, method, trick or intrigue, and finally a design or motif. To use the notion of the device is therefore to call for the simultaneous consideration of object, purpose and effect'. In our analysis of urban Jamaica, we focus on artefacts that would not necessarily all be recognized immediately as security technologies; however, within the specific contexts analyzed here, they have all been adapted for security-related purposes.
2. See, for example, Loader (2000); Dupont (2004).
3. The article draws on ethnographic fieldwork conducted by both authors in Kingston, supplemented by media analysis. Rivke Jaffe conducted a total of three months of fieldwork on the privatization and pluralization of security governance during the period 2013–2019, including interviews with a range of actors that included police and military officers, government officials, the owners and managers of private security companies, and private security guards, combined with neighborhood-level research. Francesca Pilo' conducted research on electricity governance in Kingston during five months in the period 2018–2019. This fieldwork involved interviews and participant observation in a low-income community targeted for electricity regularization, and also included interviews with a wide range of institutional actors, including employees of the electricity provider (engineers, technicians, and community relations and revenue security experts), the national electricity regulator, and urban development organizations.
4. See Bueger (2016) and De Goede (2018) for discussions of the importance of focusing on security practices.
5. However, as Pinch and Bijker point out, over time 'closure mechanisms' may generate consensus and limit such flexibility.
6. Focusing not so much on security technologies but on the broader policies and practices involved in the policing of the US–Mexico border, Peter Andreas stresses that an ostensible security policy failure is often still a political success. He argues that 'evaluating policing practices narrowly in terms of whether they attain control fails to capture their larger political and symbolic function. Border policing is not simply a policy instrument for deterring illegal crossings but a symbolic representation of state authority. . . . The powerful image effect and symbolic appeal of enhanced border policing has so far not only overshadowed its failings and flaws but made it rewarding for its architects' (Andreas, 2009: 7–8, 12).
7. For related analyses of 'failure as an instructive experience' (Lisle, 2018: 888), see Leese (2015); Molnar et al. (2019).
8. Figures obtained by searching for 'Jamaica crime rate' on the Statista website; see https://www.statista.com/statistics/984761/homicide-rate-jamaica (accessed 31 October 2022).
9. See https://www.statista.com/statistics/1040607/homicide-rate-kingston-jamaica/ (accessed 31 October 2022).
10. Much of the discussion on this specific technology is a condensed and adapted version of text included in Frossard and Jaffe (2019).
11. Eighty percent of JPS is owned privately by the Marubeni Corporation of Japan and Korea East–West Power (EWP); the government of Jamaica and a small group of minority shareholders own the remaining shares.
12. Red zones are defined as 'areas in which there are both high commercial losses and high crime rate' (Interview 1).
13. See https://jamaicaeye.gov.jm/ (accessed 29 April 2020).
14. See Ministry of National Security (2019).
15. This strategy resembles those pursued during pacification operations in Brazil; see Pilo' (2021).
16. This use is not specific to the context of Kingston: the smart grid is a technology that increasingly circulates across other urban contexts where security and commercial risks intersect (Pilo', 2021).
17. Both JPS engineers and neighborhood residents interviewed presented subcontractors as the group responsible for corrupting meters and grids in exchange for payment.
18. This type of technical failure is tolerated to a certain extent by the electricity regulator, which allows JPS to send up to three estimated electricity bills without having to compensate the affected customer (Interview 5).

19. See, for example, https://twitter.com/ChrisPinnock1/status/1285353580468342784 (accessed 6 October 2022).
20. In collaboration with key governmental agencies, JPS is currently developing the 'community renewal program', which includes the implementation of various socio-economic interventions, such as training and skill courses, wellness fairs, careers fairs, energy management sessions, etc.
21. In his work on border security technologies, Ruben Andersson (2016) similarly highlights the role of technologies in 'hardwiring' cooperation within such public–private networks of security governance.

References

Adelman RA (2018) Security glitches: The failure of the Universal Camouflage Pattern and the fantasy of 'Identity Intelligence'. *Science, Technology & Human Values* 43(3): 431–463.

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

Amicelle A, Aradau C and Jeandesboz J (2015) Questioning security devices: Performativity, resistance, politics. *Security Dialogue* 46(4): 293–306.

Andersson R (2016) Hardwiring the frontier? The politics of security technology in Europe's 'fight against illegal migration'. *Security Dialogue* 47(1): 22–39.

Andreas P (2009) *Border Games: Policing the U.S.–Mexico Divide*, 2nd edn. Ithaca, NY: Cornell University Press.

Bellanova R, Lindskov Jacobsen K and Monsees L (2020) Taking the trouble: Science, technology and security studies. *Critical Studies on Security* 8(2): 87–100.

Bigo D (2006) Security, exception, ban and surveillance. In: Lyon D (ed.) *Theorizing Surveillance: The Panopticon and Beyond*. Cullompton: Willan Publishing, 46–68.

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

Bueger C (2016) Security as practice. In: Dunn Cavelty M and Balzacq T (eds) *Routledge Handbook of Security Studies*, 2nd edn. Abingdon: Routledge, 126–135.

Campbell Y (2020) *Citizenship on the Margins: State Power, Security and Precariousness in 21st-Century Jamaica*. Basingstoke: Palgrave Macmillan.

Corsín Jiménez A (2014) Introduction: The prototype: More than many and less than one. *Journal of Cultural Economy* 7(4): 381–398.

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

Dupont B (2004) Security in the age of networks. *Policing and Society* 14(1): 76–91.

Dutta S (2009) AMI: A weapon for JPS to combat loss. *Smart Energy International*, 17 February. Available at: https://www.smart-energy.com/top-stories/ami-a-weapon-for-jps-to-combat-loss/ (accessed 6 October 2022).

Ferguson AG (2016) Policing predictive policing. *Washington University Law Review* 94(5): 1109–1189.

Ferguson AG (2019) *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: NYU Press.

Fincham R (2002) Narratives of success and failure in systems development. *British Journal of Management* 13(1): 1–14.

Frater A (2019) Sinclair upset over JPS disconnections in Flanker. *Jamaica Gleaner*, 24 July. Available at: http://jamaica-gleaner.com/article/news/20190724/sinclair-upset-over-jps-disconnections-flanker (accessed 6 October 2022).

Frossard C and Jaffe R (2019) Security and technology. In: Low S (ed.) *The Routledge Handbook of Anthropology and the City*. New York & Abingdon: Routledge, 141–152.

Gagliardone I (2014) 'A country in order': Technopolitics, nation building, and the development of ICT in Ethiopia. *Information Technologies & International Development* 10(1): 3–19.

Graham S (2011) *Cities Under Siege: The New Military Urbanism*. London: Verso Books.

Graham S and Thrift N (2007) Out of order: Understanding repair and maintenance. *Theory, Culture & Society* 24(3): 1–25.

Harriott A (2003) The Jamaican crime problem: New developments and new challenges for public policy. In: Harriott A (ed.) *Understanding Crime in Jamaica: New Challenges for Public Policy*. Kingston: University of the West Indies Press, 1–12.

Jamaica Gleaner (2019) Editorial: What is JamaicaEye seeing? 14 June. Available at: http://jamaica-gleaner.com/article/commentary/20190614/editorial-what-jamaicaeye-seeing (accessed 6 October 2022).

Jamaica Gleaner (2020) Letter of the Day: Blind JamaicaEye. 30 January. Available at: http://jamaica-gleaner.com/article/letters/20200130/letter-day-blind-jamaicaeye (accessed 6 October 2022).

Jeandesboz J (2016) Smartening border security in the European Union: An associational inquiry. *Security Dialogue* 47(4): 292–309.

Jamaica Public Service Company Limited (JPS) (2019) 2019–2024 tariff application. Kingston: JPS.

Leese M (2015) 'We were taken by surprise': Body scanners, technology adjustment, and the eradication of failure. *Critical Studies on Security* 3(3): 269–282.

Lisle D (2018) Failing worse? Science, security and the birth of a border technology. *European Journal of International Relations* 24(4): 887–910.

Loader I (2000) Plural policing and democratic governance. *Social and Legal Studies* 9(3): 323–345.

McKinson KD (2017) *Visions of the Caribbean Metropolis: Crime, Home, and the Aesthetics and Politics of Insecurity in Urban Jamaica*. PhD thesis, University of California, Irvine.

Magnet S (2011) *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham, NC: Duke University Press.

Ministry of National Security (2007) *National Security Policy for Jamaica: Towards a Secure and Prosperous Nation*. Available at: https://www.oas.org/csh/spanish/documentos/National%20Security%20Policy%20-%20Jamaica%20-%202007.pdf (accessed 6 October 2022).

Ministry of National Security (2013) *A New Approach: National Security Policy for Jamaica: Towards a Secure & Prosperous Nation*. Available at: https://japarliament.gov.jm/attachments/article/1286/1286_2014%20Ministry%20Paper%2063.pdf (accessed 6 October 2022).

Ministry of National Security (2017) *Five-Pillar Strategy for Crime Prevention and Citizen Security*. Available at: http://www.firearmlicensingauthority.com/pdf/five-pillar%20strategy.pdf (accessed 6 October 2022).

Ministry of National Security (2019) Sectoral Debate 2019/2020. Available at: https://jis.gov.jm/media/2019/04/Ministry-of-National-Security-Sectoral-Debate-2019-2020-Final.pdf (accessed 6 October 2022).

Molnar A, Whelan C and Boyle PJ (2019) Securing the Brisbane 2014 G20 in the wake of the Toronto 2010 G20: 'Failure-inspired' learning in public order policing. *British Journal of Criminology* 59(1): 107–125.

Morozov E (2013) *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: PublicAffairs.

Mosse D (2005) *Cultivating Development: An Ethnography of Aid Policy and Practice*. London: Pluto Press.

Muller BJ (2010) *Security, Risk and the Biometric State: Governing Borders and Bodies*. Oxford & New York: Routledge.

Mullings B (2019) Garrison communities. In: Antipode Editorial Collective (eds) *Keywords in Radical Geography: Antipode at 50*. Hoboken, NJ & Oxford: Wiley Blackwell, 141–145.

Pilo' F (2021) The smart grid as a security device: Electricity infrastructure and urban governance in Kingston and Rio de Janeiro. *Urban Studies* 58(16): 3265–3281.

Pinch TJ and Bijker WE (1984) The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science* 14(3): 399–441.

Radio Jamaica News (2011) Tivoli residents now on JPS tamper-proof system. 1 July. Available at: http://rjrnewsonline.com/local/tivoli-residents-now-on-jps-tamperproof-system (accessed 6 October 2022).

Shaw IG (2016) *Predator Empire: Drone Warfare and Full Spectrum Dominance*. Minneapolis, MN: University of Minnesota Press.

Smith S (2020) Police make aggressive shift in use of technology. *Jamaica Observer*, 16 February. Available at: https://www.jamaicaobserver.com/news/police-make-aggressive-shift-in-use-of-technology/ (accessed 10 October 2022).

Svensson E and Rydén A (2019) JamaicaEye: What does cybersecurity look like in one of the most recently developed CCTV networks? BSc thesis, University of Borås. Available at: http://www.diva-portal.org/smash/get/diva2:1380862/FULLTEXT01.pdf (accessed 6 October 2022).

Tironi M (2019) Prototyping public friction: Exploring the political effects of design testing in urban space. *The British Journal of Sociology* 71(3): 503–519.

Vukov T and Sheller M (2013) Border work: Surveillant assemblages, virtual fences, and tactical counter-media. *Social Semiotics* 23(2): 225–241.

Winner L (1980) Do artifacts have politics? *Daedalus* 109(1): 121–136.

Interviews cited

1. Manager of *community renewal program, JPS*, Kingston, Jamaica, *31 July 2018.*
2. Director of revenue security, JPS, Kingston, Jamaica, 2 August 2018.
3. Group interview with security company managers, Kingston, Jamaica, 26 August 2014.
4. Engineer, Revenue Security Department, JPS, Kingston, Jamaica, 7 August 2018.
5. Engineer, Office of Utility Regulation, Kingston, Jamaica, 20 May 2019.
6. Special project and logistic manager (RAMI pre-paid), JPS, Kingston, Jamaica, 18 July 2018.

Rivke Jaffe is Professor of Urban Geography at the University of Amsterdam. Connecting geography, anthropology, and cultural studies, her research focuses primarily on intersections of the urban and the political, and specifically on the spatialization and materialization of power, difference, and inequality within cities. Her current research explores the role of security dogs in mediating urban inequalities in Kingston, Jamaica. Email: r.k.jaffe@uva.nl.

Francesca Pilo' is Assistant Professor in Spatial Planning in the Department of Human Geography and Spatial Planning at Utrecht University. Her research focuses on the politics of infrastructure, studying the role of sociotechnical systems in the production of cities and in mediating the relationship between citizens and institutional actors. She has conducted extensive research in Rio de Janeiro, Brazil, and more recently in Kingston, Jamaica. Email: f.pilo@uu.nl.