The Making of Urban Computing Environments

Borders, Security and Governance

Ilia Antenucci

This paper explores the production of urban computing environments in the context of Cape Town, South Africa. It draws on research conducted between 2015 and 2017 to understand how Cape Town has been transformed into a smart city by a series of public and private initiatives.

Over the past two decades, the city has seen substantial investments in digital infrastructure, the rise of a vibrant IT industry, and the increasing datafication of urban life through smart devices, apps, and platforms, while government and corporate narratives have coined terms such as "Silicon Cape" and "Digital Gateway to Africa" to describe these shifts. In this paper, I propose two key theoretical contributions: first, I push against popular narratives of smart cities as smooth and seamless spaces, and instead point to the ways in which urban digitalization actually develops through bordering processes. Second, I describe how the governance of smart cities is informed by preemptive politics and forms of speculative security.

The paper is organized as follows. The first section examines the steps undertaken by both public authorities and private actors to develop digital technologies for the management of Cape Town. It describes the border technologies–biometric identification, algorithmic profiling, risk modeling–that operate across infrastructures, mundane objects, and devices. In pointing to these processes, and in trying to grasp their logics and effects, I work across different lines of research. These include literature on smart borders and algorithmic security (Amoore 2006; Leese 2016); critical approaches to smart cities and the making of computational environments (Kitchin and Peng 2016; Dourish 2016; Gabrys 2016); and studies on the crucial and polysemic functions of borders in the global articulation of power and economy (Mezzadra and Neilson 2013).

In the second section, I argue that smart city projects are inherently security projects, insofar as their logistic organization is informed by a logic of preemption/anticipation wherein the circulation of people and things, and "natural" resources and infrastructures become inscribed into an extensive grid of risk calculation. The extensive distribution of border techniques is instrumental to this security framework. Drawing on the work of Louise Amoore (2014) and Marieke De Goede (2012), I explore the speculative nature of security calculations based on algorithmic risk modeling. I then briefly discuss how the notions of environmental governance and biopolitics 2.0 (Gabrys 2016), and targeted governance (Valverde and Mopas 2004), might be productively integrated to analyze how preemptive politics operate. In my conclusion, I outline again the analytical and practical connections that become visible between the dissemination of border techniques across infrastructures and devices, and forms of anticipatory governance in urban computing environments.

This research moves across different disciplines and scholarships–from urban studies to security

studies, to STS– to make sense of processes that are multi-faceted, quickly shifting, and slip through any categorization. Similarly, rather than following a pre-structured design, research practices were largely inspired and crafted by my relations with the context. Semi-structured interviews with informants involved in various ways in the processes of digitalization–from city managers to security guards, from academics to IT entrepreneurs–helped me grasp the many different standpoints and agendas that inform the making of smart Cape Town, while also laying out how crucial the techniques of identification, profiling, and anticipation have become in many levels of urban life. At the same time, through the analysis of planning documents, public policies, and commercial outlets, I was able to frame the tension between smart city narratives of harmonic and seamless development, and the unfolding of bordering process throughout the new smart infrastructures.

The Borders of Digitalization

Across commercial outlets and mainstream discourses, smart cities are typically represented as smooth, seamless spaces, where the integration of computing systems with human and non-human elements makes urban life easier, safer and more sustainable for all. As Söderstrom and Klauster (2016) point out, these narratives are shaped by the commercial strategies of major firms and consultants, such as IBM, Cisco, Oracle and the like, which play a crucial role in the digitalization of cities. Digitalization has been defined as "the way many domains of social life are restructured around digital communication and media infrastructures" (Brennen and Kreiss 2016, 556). I apply this notion to the urban context to indicate the socio-technical processes through which cities are increasingly instrumented with sensing and computing systems. This section investigates the strategies of digitalization in Cape Town. It illustrates how, in contrast with popular and commercial narratives, urban digitalization actually proceeds by creating borders and disseminating border techniques across and around smart infrastructures. First, it is important to situate my argument in relation to the existing debates on, respectively, the making of digital space, and the nature and functions of borders in the present world.

Paul Dourish (2016) points to the tension between holistic design and piecemeal accumulation of technological interventions that informs urban digitalization. As Kitchin and Peng (2016) claim, code becomes materially entangled with infrastructures, services, everyday habits, and practices of government, in modalities that are always contingent. Hence, the relation between code and the city is mediated by a myriad of socio-technical assemblages which include a wide range of material and discursive elements. In her book *Program Earth*, Jennifer Gabrys (2016) delves even deeper into the making of sensing/computing environments. Drawing on Albert North Whitehead's notion of "concrescence" and Gilbert Simondon's notion of "concretization," Gabrys moves beyond the idea of assemblage as a simple addition of existing elements, and argues that sensing infrastructures and ubiquitous computation rewrite the relations between different entities, producing new forms of connection, expression, and actions. Computing environments, then, come into being through relational processes, where computing becomes environmental while at the same time, the environment becomes computational. Importantly, as Gabrys points out, this discussion of the environment strongly resonates with Foucault's notion of milieu as the setting where modes of governance unfold, and of environmentality "as a spatial–material distribution and relationality of power through environments, technologies, and ways of life" (Gabrys 2016, 187). Building on this aspect, I focus on the specific distributions of power as well as on the functions that make them visible across the urban computing environment. Borders, I suggest, are a distinct form in which power materializes and operates, and it might be particularly important to investigate the ways in which they intervene and take shape in the proliferation of sensing infrastructures.

Borders are a way to articulate power relations between humans, resources, infrastructures, and computing systems through distinct techniques, such as monitoring, identification, profiling, and risk modeling. As Mezzadra and Neilson have shown (2013), besides demarcating geographical territories, borders proliferate in various facets across and beyond national boundaries to manage the circulation of people, money, and things, and provide a privileged angle to grasp the articulation of power and capital in the global world. Borders connect and divide at once, while performing multiple and differently nuanced operations

of exclusion, classification, and filter. With the development of digital technologies, bordering processes have become more and more infused with sensing systems and algorithmic calculations. Louise Amoore (2006) has shown how biometric borders introduced in the US and Europe have proven to be inherently mobile borders that disseminate risk profiling techniques across many aspects of society. Overall, however, while pointing to the ways in which border technologies globally spread across territories, jurisdictions, labour regimes, and forms of life, the discussion so far has not specifically addressed how borders intervene in the digitalization of cities. At the same time, recent contributions analyze the effects of urban digitalization in critical terms: for example, in their study on the mega smart city of Songdo, South Korea, Halpern et al. (2016) explain how the experimentation of new sensing technologies aims to the manipulate synapsis, monetize human attention and emotions, and govern the city through automation. Shannon Mattern (2016; 2017) strongly argues against the rampant rhetoric (and projects) of cities as large-scale computers, which reduces the richness and diversity of urban intelligence to Key Performance Indicators (KPIs) and data behaviourism. Yet, these studies do not approach these socio-political issues as bordering processes– that is to say, as dynamics of demarcation, calculation, and filter across time, space, and relations. I argue that the "border gaze" can be very helpful to make sense of the effects generated by the proliferation of monitoring and profiling techniques across urban infrastructures and mundane devices. Hence, my interest here is to understand how borders become incorporated and active in the creation of urban computing environments that commonly go under the label of smart cities.

Having introduced the entanglement of bordering processes and the making of smart cities, I now move to examine how this unfolds in the case study of Cape Town. A brief look into the recent history of the city is enough to cast doubts on the idea that smart cities might develop as a seamless and harmonic environment. Cape Town is an ancient city with a complicated past. Under the apartheid regime, the urban geography was rearranged according to criteria of racial segregation, with the central and seaside suburbs made "white only," and the black and coloured population displaced into overcrowded and underserviced townships in the city's periphery. The Smart City Strategy for Cape Town[1] was launched in 2000 by the municipal government, with a strong commitment to reduce digital divide and address social inequality through IT access and services. As a first stage, the Smart Cape Access project, implemented in 2002 in partnership with IT companies Xerox and CableCom Ltd, provided free computer and Internet access in public libraries in disadvantaged areas. In 2009, the city introduced broadband fibre networks throughout the metropolitan area, and building a platform for e-governance with an estimated investment of R 1.7. billion (approximately USD 1.3 billion). Notwithstanding the substantial investments and marketing operations, the digital landscape of the Mother City remains deeply skewed. A good deal of service delivery and urban management tasks is devolved to the City Improvements Districts (CIDs): private-public partnerships funded by levies paid by property owners in a specific area. As a result, levels of digital access and integration of services differ remarkably between suburbs, depending on the economic and social capabilities of the residents. In essence, the geography of digitalization disturbingly reflects the spatial organization of the apartheid city. In the wealthy suburbs and corporate hubs, broadband networks are extensive and fast; houses and buildings are managed via IoT systems and a number of services, from parking to food delivery and payments, are provided via mobile apps. These areas are also highly securitized, with digital surveillance, electric barbed wires, and private patrols always in place. The situation is dramatically different in vast townships like Khayelithsa and Mitchell's Plain, where basic facilities such as running water or sewage are still lacking. Here, residents can only rely on a scarce number of wi-fi hotspots.[2] Access to smartphones, tablets, and laptops is limited and overall, less than 40% of the metropolitan population is able to use a computer on regular basis.[3] The distribution of infrastructures remains messy, insufficient, and contested; IT, financial, and touristic hubs are enmeshed with a "subeconomy" of informal jobs and markets, and townships and makeshifts settlements, where "old" urban poverty produced during the apartheid era and "new" poverty resulting from massive migrations from rural areas and other African countries converge.

What emerges from these examples is that in Cape Town the creation of a smart environment goes on alongside old and new bordering technologies. Far from producing a holistic and integrated environment, urban digitalization proceeds by demarcating zones, clusters, and hubs. In Cape Town, this process is mostly visible in the delimitation of informal enclaves, like the highly securitized districts for wealthy resi-

dents, or the corporate headquarters. Borders are at work around the development of digital infrastructures that are infused with spatial, economic, and racial inequalities.

As the distribution of sensing and computing technologies spread across the urban space, we can see other forms of borders taking shape. Embedded in these systems and devices are several forms of obligations, filters, and calculative practices. More specifically, I argue, smart city projects disseminate techniques that have been tested and applied in border management–real-time monitoring, biometrics identification, algorithmic profiling, and modeling–throughout mundane devices and facilities. In Cape Town, the deployment of sensing/computing networks has taken place across multiple initiatives and pilot projects that have been undertaken by the city government and maybe even more by private actors, the thriving tech start up sector in particular. As André Stelzner, Chief Information Officer (CIO) of the City of Cape Town proudly explains in a presentation (2012), in 2003, the city was one of the first in the world to implement a SAP ERP system to run every aspect of the administration into an integrated platform. Among its many features, the platform provides a single record of each citizen that identifies a person regardless of its interactions with the council. In other words, by running analytics across different data sets, the system creates a holistic profile of the citizen that covers every relevant aspect, from employment history and income levels, to potential vulnerabilities. On the basis of these algorithmic profiles, the city government is able to provide tailored services, but also to detect potential frauds or unpaid taxes.

Part of my fieldwork in Cape Town was spent observing some exclusive suburbs of the city, where the white-only doctrine is *de facto* still in place and private security guards enforce a zero-tolerance policy. Here, the houses are architectural masterpieces hovering above the ocean, and each non-white person that I saw was either a driver, a housekeeper, a garbage-picker, or a guard. CCTV systems enabled with facial recognition softwares are everywhere to identify suspicious presences, according to criteria that are explicitly biased. After some hard pressing and repeated promises of anonymity, I managed to interview one of the private security officers in charge of the area. A white, middle-aged man, with a past in the South African Special Forces, he explains[4] that they "obviously (*sic*)" target young black individuals "who have no properties, and therefore no business in the area, except causing troubles *(sic)*."

The association of border techniques and instruments of digital surveillance does not come as a surprise, but practices of identification and profiling are at work well beyond the field of security. Since 2015, Cape Town has been facing the worst water crisis in its history, as the dams were at their lowest in a century and the menace of Day Zero–the day when taps would have to be shut off–was looming. Among other severe water restrictions, smart water meters have been installed to optimize the management of resources. Connected through IoT networks, and managed via mobile platforms, smart meters monitor real-time water usage for each user, detect and report anomalous events such as leaking, and create profiles of consumption. Now that the crisis seems to have been contained, or at least postponed,[5] smart meters are celebrated as a game-changer.[6] As planning documents[7] illustrate, the City is working towards increased automation of the water system–that is, the control and reading of meters via IoT devices, and the use of analytics to develop proactive strategies.

Having lived for a few months in the central areas of the city, I also experienced how an increasing number of utilities and everyday activities are managed, sometimes exclusively, via mobile platforms. Uber car rides, carpooling, meals and grocery delivery, cashless payments, booking restaurants or gym classes, buying tickets for concerts or exhibitions, pre-ordering my coffee to skip the queue, finding a parking lot, checking the weather forecast, load shedding schedule, and shark spotting, were only some of the app-based services where I–as well as most people I knew there–signed in. In my almost five months in Cape Town, I registered at least twenty profiles, and would use them between twenty five and fifty times a day.

These examples of digital practices and habits from different domains illustrate how, despite the lack of a single, holistic masterplan, large portions of Cape Town and urban life are extensively enabled with sensing technologies and contribute to massive computations. Again, these operations take place by disseminating techniques of monitoring, identification, and profiling across mundane facilities and devices. The information remains dispersed among different actors, many of which are private companies. Via its SAP platform, the city government uses predictive analytics to re-calibrate the delivery of services and governance, while also hosting an Open Data portal. Simultaneously, though, massive amounts of urban data

are algorithmically processed and modelled privately, as part of corporate business operations. In addition to this, the distribution of sensing technologies reinforces existing borders, and often create new ones, along class and racial lines, spatial hierarchies, and access to resources.

In the above examples, the promise of a harmonic, seamless smart city breaks into a landscape of ubiquitous border techniques that are active *around* and *across* the sensing systems, and that incessantly scrutinize and filter bodies, identities, and movements. At once, access to digital infrastructure becomes compulsory in order to receive essential services and information, and conditional to the requirements embedded in the computing systems. Borders materialize and operate in different modalities. On one level, access to digital infrastructures is, to some extent, physically restricted: think of the walls and security systems that protect the highly privatized IT hubs of the city. On a second level, digital infrastructures become the border themselves, insofar as they monitor and restrict the movements of people, as it is the case for smart surveillance cameras targeting specific groups or behaviours. A third level of borders concerns the extensive deployment of profiling techniques across infrastructures and devices, whereby access to services is filtered (e.g., water consumption) and "tailored" policies are crafted. These type of borders are apparently immaterial, as they do not coincide with any physical location; yet they are pervasive, and have very material effects on the life of those who encounter them. The simultaneous presence of public and private actors in the management of data generates further filters and limitations to the ways in which data are processed and used. Last but not least, a further level of borders to take into account in the digitalization of cities are those specific to the type of algorithms and code strings employed in the softwares that process urban data sets. there is no mention in any public documents within the Cape Town administration of the analytics settings employed in their softwares. The type of inferences in use–whether analytics are based on predictive, descriptive, or decision models, which pools of data they elaborate, and across what time range–all these formulas remain undisclosed, protected by copyright and corporate policies, as well as by sophisticated cyber-security programs. This is especially so in the case of private companies. It is therefore impossible for common citizens to know the criteria according to which urban information is being analyzed, and on the basis of which decisions with public consequences are made. Importantly, the different levels of borders described above are not temporally or hierarchically ordered, but work simultaneously and often in entanglement. While challenging the usual notion of border as a physical demarcation between territories, they show how border logics and practices–monitoring, profiling, filtering, blocking–are inherently active through the new urban technologies. Furthermore, they have immediate effects on the ways in which risks are identified, and urban government and security are managed.

Smart Cities as Security Projects

Urban computing environments–smart cities–are intrinsically security projects. This is not generally the case because they are planned as massive surveillance systems, as part of smart city critics argue (Kitchin, 2014; Tufeckci, 2014). Of course monitoring is an important feature of computing networks, but not one that captures their sense overall. Smart cities, I suggest, are security projects because they are informed by a logic of anticipation and preemptive risk management. The dream of smart city planners is indeed that of a city where every movement and every disruption can be calculated and acted upon in advance. The dissemination of border techniques throughout urban infrastructures and mundane objects serves precisely this rationale: to set up an extensive grid of measurement onto which models can be projected.

It has been observed that border techniques of identification, profiling and modeling take part in a turn towards preemptive or anticipatory governance that can be observed across many fields, from disaster management to anti-terrorism and policing (Amoore 2013; De Goede, Simon, and Hojitnik 2014). In his seminal article "Preemption, Precaution, Preparedness: Anticipatory Action and Future Geographies," Benedict Anderson (2010) identifies preemption as one of the logics of anticipatory action–together with precaution of preparedness–whose specificity is that it works on undetermined, potential scenarios of the future. Largely shaped by the aftermath of 9/11, when security officers and policy-makers were shockingly compelled to focus on "low-probability, high-impact" events, preemptive governance has increasingly

sought to incorporate the imagination of future possibilities into risk calculations and security procedures. The nature of security practices has then become *speculative*, as it no longer settles for probabilistic evidence, but strives to grasp the unknown, the improbable, and the multiple possible futures, into present decisions. As De Goede, Simon and Hojitnik note, security is speculative "not because it is imaginative or unreal, but because it deploys notions of futurity that parallel the technologies of financial speculation. Like financial speculation, preemption is not so much about predicting the future, but acts on multiple potential futures that are rendered actionable (or liquid) in the present" (2014, 413, drawing on Cooper 2010; De Goede 2012; Amoore 2013). As Anderson puts it, preemption is "generative" as it unleashes transformation and unlocks opportunities in the present (2010, 790). Operations of speculative security can be understood across different practical and theoretical dimensions. On the one hand, security practices increasingly rely on algorithm-based, so-called "predictive" analytics, whose characteristics are important to understand how security knowledge–risk scores, risk models, alerts–is achieved. For example, non-obvious relationship awareness (NORA) softwares, developed in a commercial context and then largely employed for border management and law enforcement, are able to unearth meaningful connections and patterns across large volumes of different data sets–demographics, financial transactions, social networks and web surfing, mobile phone data, criminal records, etc.–and then aggregate the relevant information into individual profiles. At the same time, machine learning algorithms are increasingly being experimented with. They automatically create profiles and models while being able to re-generate their own settings, with minimal human intervention. Albeit commonly labeled as a whole as "predictive analytics," the types of analytic models used in commercial and government sectors are in fact various and differently structured. Predictive models, which analyze past records to predict how likely an individual or object is to have a specific behaviour in the future, are used to create individual risk scores, like credit rating. Descriptive models, whose target is to identify relationships between groups of people (or objects), allow to create categories of threats, such as no-fly lists. Decision models, commonly considered the most advanced level of predictive analytics, are able to predict the outcome of a complex situation, taking into account the results of predictive and descriptive models as well as broader contextual factors; for example, the appropriate number of firefighting equipment to deploy in a high-risk day, and in what sites to prevent fires from spreading. Differently and flexibly configured, all these families of computing operations do not actually predict anything. Rather, they are somehow able to think, or at least operationally speculate on the endless contingencies of big data, to draw out meaningful results and even make decisions. In this sense, algorithmic prediction is, in fact, speculation.

On the other hand, as De Goede (2012) demonstrates in her research on the pursuit of terrorist money, security is speculative insofar as material security interventions, including analytics and risk modeling, only become possible when a visual field is created, which inevitably includes assumptions, ideals, emotions, and objectives, and is therefore politically charged. As poignantly noted in a more recent work, "algorithms do not deliver fully automated security judgements. They need instructions concerning risk appetites, patterns, and thresholds. Furthermore, software systems are integrated into wider professional environments, leading to processes of appropriation that are situated and to some extent unpredictable" (De Goede 2017, 40).

The making of urban computing environments offers distinct possibilities to observe speculative security in action. In 2017, the City of Cape Town launched an integrated solution called EPIC (Emergency Policing and Incident Command), that incorporates six public safety departments–fire and rescue, traffic, metro police, law enforcement, disaster risk management, and the special investigative unit–into a single control platform.[8] Powered by SAP HANA system, EPIC relies on an IoT network made of GPS trackers, cameras, mobile apps, fire detectors etc., that connects every human and non-human component of the emergency services, from ambulances to policemen to fire hydrants. In the central command and control room, real-time data are displayed in dashboards and interactive risk maps, that allow staff to have a holistic gaze on the city's security status. Real-time monitoring, improved response, and coordination of the interventions are described as key improvements achieved through the new system. However, according to developers and officers, the real game-changer in EPIC is the business intelligence layer, where analytics are at work. On one hand, analytics process data sent in from the sensing networks to produce instantaneous decision models. Algorithms elaborate whether an incident is happening or not, classify the event in order

of importance and severity, calculate what type and number of resources are needed and in what time. But even more importantly, analytics work on the future. Information about each incident, including video and photo reports, number of victims, number and type of resources employed, cost of the intervention, are recorded in the system for further analysis. By aggregating data and creating automated reports, EPIC is able to produce models of different categories of risks and emergencies, as well as automated protocols that apply to different cases. Continuously updated through the algorithmic feed, these models indicate how to optimize resources, assign risk scores to specific associations of criteria, and describe what a risk alert might look like. In spite of their commercial label, predictive analytics and models do not actually *predict* anything, as no mathematical operation is able to say when and where exactly an incident will occur; instead, they offer a range of configurations of the future upon which anticipatory action can be taken. In this sense, EPIC analytics work in a speculative manner, arranging possibilities, uncertainties, and options into specific formats. At the same time, as noted before, these analytics do not operate in a neutral vacuum, but are instructed with settings and criteria that are always materially and politically situated, and include some degree of bias that informs the very definition of risk and emergencies. In Cape Town, for example, the propension to fire hazards, the scarcity of water, the limited budget available for emergency management, the presence of deprived areas with high crime rates are some of the factors that guide the operations of EPIC analytics. As a result, EPIC works at the interface between human and automated speculation to translate the city in the language of risk. Presented as a superior form of knowledge, these speculative syntheses become the foundation for preemptive initiatives of urban security. Decisions as to where and when to concentrate resources, which areas or groups of people should be kept under scrutiny, which departments should have their budgets slashed or increased, are taken on the basis of models, in the attempt to be prepared for potential emergencies, and to minimize the risk scores.

In examining the distinct ways in which urban preemptive politics unfold, I take up two analyses of the evolutions of government that might be productively combined. One is the notion of environmental governmentality sketched out by Michel Foucault at the end of his lectures on *The Birth of Biopolitics* (2008), and has been recently discussed by Jennifer Gabrys in her study on ubiquitous computing and urban governance (2016). The other one is the idea of targeted governance formulated by Mariana Valverde and Michael Mopas (2004). By pointing to environmentality, Foucault was drawing attention to the ways in which biopolitical techniques and modes of regulation were increasingly shifting from subjects and population to the broader conditions of life. The focus of government, Foucault suggested, was no longer so much on "players"–individual or collective behaviours–but rather on the "rules of the game"–the "milieu," the environmental setting–that make behaviours possible or impossible. Gabrys moves from this formulation, which Foucault never developed further, to engage with the increasing implementation of computational technologies in urban environments, and their effects in terms of government. Trying to grasp more deeply how the distribution of power operates through computing environments, Gabrys introduces the notion of *biopolitics 2.0* as an analytical tool "to examine specific ways of life that unfolds within the smart city" (2016, 190-92). At the same time, I suggest, this notion illuminates some key features of preemptive governance and security in the smart city. As found in the examples above, (speculative) preemption and security work by trying to anticipate and reshape the rules of the game in advance, dragging a projection of potential future risk into the present, as a terrain of intervention. In this sense, preemption and security are inherently modes of environmental governmentality and biopolitics, as they translate life conditions into the grammar of risk, and try to act on them through specific knowledge techniques, such as mapping, trakking, monitoring, measuring, profiling, and modeling. Yet, and apparently in contrast with the idea of environmental governance, speculative security/preemption can be linked to the idea of targeted governance. This is described by Valverde and Mopas (2004) as a burgeoning shift in governmental practices across different fields–from criminal justice and policing to healthcare, insurance and social security, immigration and border security–where interventions on individuals or categories of people are based on accurate risk calculations are presented as smart and free from side-effects. Targeted governance breaks up its objects "into a set of measurable risk factors" (Valverde and Mopas 2004, 240), which are then recombined into patterns of security action.

We have observed a very similar mechanism in the work of the speculative analytics model for

urban security decisions. With the development of ubiquitous computing systems, smart cities and citizens are increasingly inscribed into processes of risk profiling and modeling that measure the activities of individuals and categories of people, as well as their relations with the urban infrastructures and resources. I described before how the ERP software for the urban management of Cape Town generates individual profiles of citizens and targeted policies of various natures, from tax inspections to police controls or social benefits. At the same time, a system like EPIC is able to extend this risk profiling and modeling mechanism to a broader range of objects, including resources, like water, events, or areas of the city. My point here is that, albeit seemingly alternative, environmental governance and targeted governance are an actually simultaneous and deeply intertwined articulation of urban preemptive politics. Techniques of security speculation embrace at once the infrastructural and environmental conditions within which the city lives, and the microscopic, intimate ways in which singular forms of life unfold. The distinction between humans and non-humans components of the smart city fades, as long as it is possible to register each element into risk calculations and processes of speculation on the future.

Conclusion

This paper has examined the transformation of Cape Town into a smart city, drawing attention to some key processes and tendencies in the urban government. In the first section I have illustrated how, in contrast with mainstream and commercial narratives of smart cities as smooth, seamless environments, urban digitalization actually proceeds by establishing zones and borders. On the one hand, borders are *visible* around the uneven spatial distribution of digital infrastructures, which reflects and reinforces economic and racial inequalities. The highly securitized digital hubs of the city are only accessible to wealthy residents or corporate workers, while most of the townships remain digitally underserved and public wifi does not even nearly cover the demand. As a result, despite the emphasis on Cape Town's smartness, large sectors of the urban population–especially the black population–are *de facto* excluded from, or only gradually included, into the digital developments. At the same time, borders operate *across* the proliferation of urban computing systems, as techniques of monitoring, identification and profiling become increasingly embedded in all sorts of mundane objects and devices, and put in place new types of filters, obligations and calculative practices. Water provision is restricted if the smart meter signals excessive consumption. Social payments are suspended if the SAP algorithm identifies a potentially fraudulent profile. Anyone walking around the city can be stopped and questioned if her face matches the (often biased) recognition settings of smart camera. Jennifer Gabrys observes that sensing and computing environments are able to rewrite the relations between human and non-human elements, and generate new forms of life. Building on this, I suggest that focusing on bordering processes is a way to grasp the distribution of power through these relations, as the examples above indicate.

The second section of this paper has argued that smart cities are inherently security projects. In saying this, I do not refer to the aspects of surveillance that part of the critique emphasizes. Instead, I suggest that while surveillance is definitely one important aspect of urban computing systems, what makes smart cities security projects is the fact that they are informed by a logic of anticipation and preemptive risk management. At least on paper, a smart city is a fully programmable environment, where any potential disruption can be known and acted upon in advance. The extensive dissemination of border techniques across the urban space enables the incessant collection of data on the basis of which risk models are generated. These are based on algorithmic operations that draw connections among large volumes of data on the basis of contextual settings or machine learning, while trying to identify meaningful patterns. Albeit presented as evidence-based predictions, risk models are actually highly speculative as they only provide distinct configurations of the future. Yet, as the example of the EPIC system for emergency management shows, these models become the grounds for security decisions with having a high impact on the public. In discussing the proliferation of border techniques and risk modeling I take up the concepts of environmental governance (Gabrys 2016) and targeted governance (Valverde and Mopas 2004). Although formulated in a different context and in a seemingly alternative way, I suggest these two interpretations of governmental evolutions are deeply interrelated and simultaneously at work in the government of urban computing

environments, where the logic of risk calculation absorbs human and non-human components, individual, and systemic processes at once.

While this article is based on empirical research conducted in Cape Town, it describes processes and tendencies that are by no means exclusive to this case study. Techniques and operations reviewed here can be observed, at different scales, in many smart city projects across the globe. It is well-known that from Chicago to Barcelona, from Amsterdam to Tokyo, IoT networks, and the monitoring and profiling techniques attached to them, are increasingly taking over infrastructures and service provision. Softwares that are very similar to EPIC in structure and scope have been adopted by a number of cities to manage logistics and emergencies, such as the Operations Center of Rio de Janeiro, run on IBM systems, or the Safe City Solution in Singapore, developed by Accenture.[9] Each of these cases requires a situated investigation and specific empirical attention before a common framework can be formulated; yet, I suggest that bordering processes and preemptive politics might provide one theoretical avenue, among others, to develop critical understanding of urban digitalization in its global dimension.

References

Amoore, Louise. 2006. "Biometric Borders: Governing Mobilities in the War on Terror." *Political Geography* 25: 336-351.
Amoore, Louise. 2013. *The Politics of Possibility: Risk and Security Beyond Probability*. Durham, NC : Duke University Press.
Anderson, Benedict. 2010. "Preemption, Precaution, Preparedness: Anticipatory Action and Future Geographies." *Progress in Human Geography* 34 (6): 777-798.
Brennen, J. Scott, and Kreiss, Daniel. 2016. "Digitalization." In *The International Encyclopedia of Communication Theory and Philosophy*. Malden, MA : Wiley Blackwell
de Goede, Marieke. 2012. *Speculative Security the Politics of Pursuing Terrorist Monies*. Minneapolis: University of Minnesota Press.
de Goede, Marieke, Stephanie Simon and Marijin Hojitnik. 2014. "Performing Preemption." *Security Dialogue* 45: 411-422.
Dourish, Paul. 2016. „The Internet of Urban Things." In *Code and the City*, edited by Rob Kitchin and Sung-Yueh Perng, 27-46. London: Routledge.
Foucault, Michel, A. Davidson, and G. Burchell. 2008. *The Birth of Biopolitics: Lectures at the Collège de France, 1978-1979*. Basingtsoke : Palgrave Macmillan UK.
Gabrys, Jennifer. 2016. *Program Earth: Environmental Sensing Technology and the Making of a Computational Planet*. Minneapolis: University of Minnesota Press.
Halpern, Orit, Jesse LeCavalier, Nerea Calvillo, and Wolfgang Pietsch. 2016. „Test-bed as Urban Epistemology." In *Smart Urbanism : Utopian Vision or False Dawn?*, edited by Simon and Luque-Ayala Marvin, Andrés and McFarlane, Colin, 146-168. London; New York: Routledge.
Kitchin, Rob. 2014. „The real-time city? Big data and smart urbanism." *GeoJournal* 79 (1):1-14.
Kitchin, Rob, and Sung-Yueh Perng. 2016. *Code and the City*. New York: Routledge
Leese, Matthias. 2016. „Exploring the Security/Facilitation Nexus: Foucault at the 'Smart' Border." *Global Society* 30 (3): 412-429.
Marvin, Simon, AndrÈs Luque-Ayala, and Colin McFarlane. 2015. *Smart Urbanism*. Florence, UNITED STATES: Taylor and Francis.
Mattern, Shannon "Instrumental City: The View from Hudson Yards, circa 2019." *Places Journal*. https://doi.org/10.22269/160426, last access February 27, 2019.
Mattern, Shannon "A City Is Not a Computer." *Places Journal*. https://doi.org/10.22269/170207, last access February 27, 2019.
Mezzadra, Sandro, and Brett Neilson. 2013. *Border as Method, Or, the Multiplication of Labor*. Durham NC : Duke University Press.
Söderström, Ola, Till Paasche, and Francisco Klauser. 2014. "Smart cities as corporate storytelling." *City* 18 (3): 307-320.
Tufekci Zeynep. 2014 "Engineering the Public: Big Data, Surveillance and Computational Politics." *First Monday* 19 (7).
Valverde, Mariana, and Mopas Michael. 2004. "Insecurity and the Dream of Targeted Governance." In *Global Governmentality: Governing International Spaces*, edited by W. Larner and W. Walters. London: Routledge.

Endnotes

1 See http://acceleratecapetown.co.za/wp/wp-content/uploads/2016/11/The-City-of-Cape-Towns-Digital-Journey-Towards-a-Smarter-Future-Rudy-Abrahams-CoCT.pdf, last access February 27, 2019.
2 See https://www.westerncape.gov.za/general-publication/switching-public-wi-fi-hotspots-across-western-cape, last access February 27, 2019.
3 See http://www.capetownpartnership.co.za/2017/04/datamustfall-backhaul-bottle-necks-expose-sas-digital-economy/, last access February 27, 2019.
4 Interview taken in Cape Town, October 2015.
5 See https://qz.com/africa/1272589/how-cape-town-delayed-its-water-disaster-at-least-until-2019/, last access February 27, 2019.
6 See http://acceleratecapetown.co.za/smart-meters/, last access February 27, 2019.
7 Seehttp://resource.capetown.gov.za/documentcentre/Documents/City%20strategies,%20plans%20

and%20frameworks/WCWDM_Strategy_doc.pdf, last access February 27, 2019.

8 See https://www.sap.com/africa/about/customer-testimonials/finder.html?tag=industry:public-sector&search=cape%20town&sort=latest_asc, last access February 27, 2019. See also https://www.itweb.co.za/content/6mQwkoq6Z2Gq3r9A, last access February 27, 2019, and http://www.afsug.com/library/documents/saphila_2017_presentations/STREAM%202_P03_Alderman%20JP%20Smith%20Andrew%20Mortimer.pdf, last access February 27, 2019.

9 See https://www.accenture.com/t20180328T090722Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Industries_13/Accenture-Singapore-Government-Safe-City-Test-Bed.pdf, last access February 27, 2019.