Edwards and Calaresu *City Territ Archit* (2018) 5:19
https://doi.org/10.1186/s40410-018-0089-1

City, Territory and Architecture

EDITORIAL Open Access

Smart cities and security: Editorial preface

Adam Edwards[1*] and Marco Calaresu[2]

Emergent technologies, sometimes referred to as Disruptive Digital Technologies (DDTs), including social media, machine-learning, 3-D printing, advanced robotics, unmanned vehicles (drones) and the Internet of Things (IoT), provoke argument over the opportunities for realising "smart cities" but also the threats of introducing new vulnerabilities into the governance and security of city-regions. Given the rapid evolution of these technologies and uncertainty about their likely impact, this special issue invited contributions of a conceptual, methodological and/or empirical focus that consider how social science can better understand and respond to the opportunities and threats of smart cities.

The "smart city" is promoted as an unqualified positive development, particularly given pressures for more efficient, economic and effective governance in rapidly expanding cities. However, in the dash for technological fixes to the various pressures of urbanisation, there is a tendency to overlook the security implications of "smarter" critical infrastructure, including its vulnerability to criminal enterprise and terrorist attack. Such reflection is especially pressing if, as suggested by some (Omand 2016), both commercial and governmental dependence on the internet has gone "past the point of inflexion" in the United States as well as in many European countries, and as the migration of critical infrastructure on-line has the potential to accelerate the sociotechnical "arms race" between organisers and preventers of serious crime.

The "WannaCry" ransomware attack of May 2017 exemplifies the kind of vulnerabilities that can arise from the dependence on Internet-enabled critical infrastructure envisaged by advocates of the smart city. Amongst its other global effects, this attack compromised a third of English National Health Service information systems over a 72-h period, resulting in the cancellation of 20,000 appointments and operations (Boiten and Wall 2017). Subsequent investigation attributed this to the vulnerability of those healthcare authorities who had not upgraded their obsolete IT operating systems, such as Windows XP, which Microsoft had withdrawn support from 3 years prior to the attack (Dwyer 2018). This and countless other human decisions left unpatched operating systems vulnerable to a relatively unsophisticated virus, indicating the brittle security of critical infrastructure in smart cities.

Beyond such exceptional instances of the insecurity of smart cities as the WannaCry attack, it is possible to envisage the proliferation of more mundane and quotidian vulnerabilities. Public policy is, for example, increasingly preoccupied with the vulnerabilities of young people to harmful, every day, social media communications and their alleged impact on mental health and wellbeing (Webb et al. 2015; Housley et al. 2018). Another mundane security concern is the increasing connectivity, and thus vulnerability to hacking, of household appliances through the Internet of Things (IoT). If such threats can be characterised as "new opportunities for new types of crime", or "true cybercrimes", that couldn't exist without the internet, it is also possible to envisage how internet connectivity can "assist existing or 'ordinary' crime", as in the augmentation of the illicit trade in drugs using mobile smart phones (Wall 2010). Smart cities might also facilitate the proliferation of "hybrid cybercrimes" or "new global opportunities for existing or 'traditional' crimes", such as the distribution of extreme pornography across borders (Wall 2010). In these more expansive terms, smart cities and their vulnerabilities are already ubiquitous in continents where Internet usage is estimated at over half of the population (Smith et al. 2015).

Given this ubiquity and mindful of the orientation of this journal, the special issue invited reflections on how emergent technologies can alter our understanding of

*Correspondence: EdwardsA2@cardiff.ac.uk
[1] Cardiff University, Cardiff, UK
Full list of author information is available at the end of the article

what constitutes the territory and architecture of security, and how public authorities are making sense of the challenges presented by emergent technologies for urban governance. A central challenge of smart cities in the twenty-first century is how they disrupt conventional concepts of territory and architecture associated with the built environment of offline social relations. Given the ubiquity of Internet usage, certainly in the developed world, it is becoming harder and less conceptually relevant to bracket-off such offline social relations from the disruptive effects of online technologies. Rather, the territorial aspects of security need to be understood in terms of the increasing penetration—and consequences—of the "ether" into civil society, the governance of urban life and public policies. A corollary of this is that concepts of the architecture of security in such cities need to extend beyond the familiar connotations of human-shaped *terra firma*. They also need to encompass the architecture of cyberspace, from the predatory interactions on "second life" (Williams 2007) and other avatar-based social relations, including the nascent "virtual nightclub" (Berry in this issue), to the "choice architecture" of various social media platforms and how these might enable or frustrate victimisation through "trolling" or abusive, defamatory, communications.

In these terms, sociology, criminology and political science (with particular reference to public policy analysis) have much to offer the reconceptualisation and investigation of security in smart cities given the current need to transcend the built-environmental concepts of crime and the city found, e.g., in the legacy of the Chicago School with its understanding of cities as self-contained residential "zones" that are more or less criminogenic (Shaw and McKay 1942); or in Mike Davis' "ecology of fear" in late-twentieth century Los Angeles (Davis 1998).

This special issue represents an initial attempt at importing sociological, criminological and political concepts into arguments about security in smart cities.

The issue opens with our own contribution (Edwards and Calaresu in this issue) on official narratives of security in which we argue, by means of a semi-automated approach to the analysis of narrative data, that smart cities have, hitherto, remained conspicuous by their absence in governmental accounts of contemporary threats. The contribution relates the narrative analysis to broader arguments about the significance—both in terms of the politics and policy—of city-regions as objects of security. The concept of the "smart city" is privileged in commercial attempts to promote technological solutions to problems of urban governance but with negligible reflexivity about the potential vulnerabilities that these "solutions" are themselves liable to create. At the risk of sounding overly conspiratorial, it can be conjectured that this limited consideration of the security implications of smart cities in official and commercial narratives reflects a coincidence of interests between Tech companies seeking to market their products and municipal administrations who are, in turn, struggling with the increasing pressures of urbanisation. This struggle is especially acute in those city-regions subject to austere cuts in public expenditure in the decade since the financial crisis of 2008.

In turn, this provokes further questions for debate about the utility of the concept of the "smart city", when shorn of its commercial qualities. Here it is possible to identify accounts that are off-line-centred, as in Schuilenburg and Peeters' contribution to this special issue, on the "de-escalate project" in the Dutch city of Eindhoven, and those that are online-centred, as in Poletti and Michieli's study of attempts to regulate social media communications that have the potential to fuel offline conflicts, as exemplified in the case of attacks on the office of the satirical magazine, *Charlie Hebdo*, in Paris in February 2015 (Poletti and Michieli in this issue).

Schuilenburg and Peeters develop the innovative argument that smart cities can advance a form of "pastoral power" which is genuinely concerned to govern behaviour through "care and protection" rather than punishment and exclusion (Schuilenburg and Peeters in this issue). This is evidenced through reference to the use of automated audio-visual sensors in Eindhoven's night-time economy. These illuminate crowded spaces and broadcast ambient music when raucous behaviour is sensed, on the basis of evidence suggesting crowds are pacified in harshly lit environments and through a more subdued tempo of music. In this instance, off-line behaviour is being regulated by an online architecture of automated censorship algorithms that are, themselves, informed and refreshed by cumulative evidence on crowd management experiences in other night-time economies.

Poletti and Michieli's contribution discusses the consequences of the attack on the office of Charlie Hebdo on debates over the need for a greater regulation of online social media communications, given their potential to stimulate offline urban violence. It employs the novel methodology of "controversy mapping" to discuss the online/offline interface in smart cities as a site of conflict and controversy. As such, this contribution foregrounds relations of power and political activism in the "actor-networks" that constitute and reproduce smart cities.

In his contribution, Berry further extends the actor-networks involved in the constitution of smart cities to include those interested in exploiting their vulnerabilities. He argues that any programme of research into threats to the security of smart cities needs to investigate what this concept can mean to these actors, although

hitherto the perceptions of criminal entrepreneurs have been conspicuous by their absence in controversies over the meaning and consequences of smart cities. By contrast, Berry illustrates the crucial insights to be gained from understanding these perceptions through reference to his ethnographic investigation of the use of smart technologies to augment the operation of illicit drug markets and how internet-enabled communications can be used to deceive and outflank security actors. He argues that in the absence of insights into the perceptions of criminal entrepreneurs, public debate will be reduced to recycling official and commercial preconceptions of what constitute insecurities in smart cities, resulting in self-referential policies on how they ought to be addressed.

McGuire further deepens criticism of official and commercial accounts of smart cities for their failure to grasp the unintended consequences of technologies that produce "stupid citizens" (McGuire in this issue). In a development of Richard Sennett's anarchistic critique of overly controlled urban life, McGuire posits a teleology of smart cities in which so much human agency is filleted out of everyday decisions, especially the opportunity to make mistakes, to get lost but to be surprised and discover things as a consequence, that citizens lose the capacity for citizenship. The terminus of this telos is a bleak stultification in which over-regulated human beings lose the will and inclination to govern themselves, including the ingenuity needed to adapt to ever evolving and uncertain insecurities.

A common thread throughout the papers in this special issue is the interaction of humans and machines that is now, surely, a central and defining characteristic of the territory and architecture of security in the cities of the digital age (Edwards 2016, 2017). Purported tendencies of this interaction, toward the enlightened, "pastoral", care and protection of citizens, their stupefaction and ultimate insecurity or their ingenuity in public controversies over online control or in criminal entrepreneurship, alert us to the importance of the dilemmas inherent in securing smart cities. In this evolving research programme, it would be unwise to overestimate the powers of machines or to underestimate the capacity of humans for resistance and improvisation in "democratic cities" (Tebaldi and Calaresu 2015), which Robert Dahl already considered, more than 50 years before they became "smart cities", as having the "greater claim" than any other territorial alternative to becoming the "optimum unit for democracy in the twenty-first century" (Dahl 1967).

Authors' contribution
This article is the result of a joint effort undertaken by the two authors. Both authors read and approved the final version of the manuscript.

Author details
[1] Cardiff University, Cardiff, UK. [2] University of Sassari, Sassari, Italy.

Competing interests
The authors declare that they have no competing interest.

Publisher's Note

Published online: 07 November 2018

References

Boiten EA, Wall DS (2017) WannaCry report shows NHS chiefs knew of security danger, but management took no action. In: The Conversation. https://theconversation.com/wannacry-report-shows-nhs-chiefs-knew-of-security-danger-but-management-took-no-action-86501. Accessed 13 Sept 2018

Dahl RA (1967) The city in the future of democracy. Am Political Sci Rev 61(4):953–970

Davis M (1998) Ecology of fear: Los Angeles and the imagination of disaster. Macmillan, London

Dwyer A (2018) The NHS cyber-attack: a look at the complex environmental conditions of WannaCry. RAD Magazine 44:25–26

Edwards A (2016) Multi-centred governance and circuits of power in liberal modes of security. Global Crime 17(3–4):240–263

Edwards A (2017) Big Data, Predictive Machines and Security. In: McGuire MR, Holt TJ (eds) The Routledge handbook of technology, crime and justice. Routledge, Abingdon, pp 451–461

Housley W, Webb H, Williams M, Procter R, Edwards A, Jirotka M, Burnap P, Stahl BC, Rana OF, Williams ML (2018) Interaction and transformation on social media: the case of Twitter campaigns. Social Media and Society 4(1):1–12

Omand D (2016) Plenary address. Third Winchester conference on trust, risk, information and the law, University of Winchester, Winchester, 27th April 2016

Shaw CR, McKay HD (1942) Juvenile delinquency and urban areas. University of Chicago Press, Chicago

Smith RG, Chak-Chung Cheung R, Yiu-Chung Lau L (eds) (2015) Cybercrime, risks and responses. Palgrave, London

Tebaldi M, Calaresu M (2015) "Democra-city": bringing the city back into democratic theory for the 21st century? City, Territ Archit 2(13):1–15

Wall DS (2010) The Internet as a conduit for criminals. In: Pattavina A (ed) Information technology and the criminal justice system. Sage, Thousand Oaks, pp 77–98

Webb H, Jirotka M, Procter R, Stahl BC, Housley W, Edwards A, Williams ML, Burnap P, Rana OF (2015) Digital wildfires: hyper-connectivity, havoc, and a global ethos to govern social media. Comput Soc 45(3):193–201

Williams ML (2007) Avatar watching: participant observation in graphical online environments. Qualitative Res 7(1):5–24