Creating Smart Cities; edited by Claudio Coletta, Leighton Evans, Liam Heaphy and Rob Kitchin
Format: Royal (156 × 234 mm); Style: Supp; Font: Bembo;
Dir: W:/2-Pagination/CREAT_RAPS/ApplicationFiles/9780815396246_text.3d;

16

THE CHALLENGES OF CYBERSECURITY FOR SMART CITIES

Martin Dodge and Rob Kitchin

Introduction

Over the past three decades there has been a concerted move to digitally augment existing infrastructures, roll out new networked infrastructures, and utilize computational systems to tackle urban problems and deliver city services more efficiently. Such endeavours are now encapsulated within the notion of "smart cities", which advocates claim can help address urban resilience and sustainability in a time of population increases, climate change, and deepening socio-economic inequalities (White, 2016). In other words, smart city technologies are seen to offer an effective way to counter and manage uncertainty and risk. However, as with previous rounds of technological adoption and adaptation in cities – such as those related to energy supply, transportation, and telecommunication – they also create a paradoxical situation wherein the promised benefits (such as convenience, economic prosperity, safety, sustainability) are almost always accompanied by negative consequences and new variances of traditional problems (e.g., reproducing inequality, creating security and criminal risks, environmental externalities) (Greenfield, 2013; Singh and Pelton, 2013; Townsend, 2013). Importantly, this paradoxical relationship and the reproduction of urban problems and risks in a new guise is for the most part ignored in the promotional discourse for smart cities driven by commercial and governmental interests, or is present as a potential new issue to be "solved" by a further round of technological innovation and capital spending.

This chapter examines the implications of this paradoxical relationship, detailing how smart city technologies designed to produce urban resilience and reduce risks are actually opening up systems they are meant to augment to new forms of vulnerability and risk. The discussion considers the balancing point between reward and risk when previously relatively "dumb" systems are made "smart" through the introduction of networked computation, and are thus opened up to software bugs,

data errors, network viruses, hacks, and potential criminal and terrorist cyberattacks (Little, 2010; Cerrudo, 2015).

For as long as there have been urban societies there have been criminal activity and attempts to steal property, disrupt city infrastructure, and defraud public services. Attempts to thwart such criminality have been built into the fabric of cities themselves through architecturally enacted defences, strong doors, high walls and fences, and latterly security alarms and CCTV. Historical evidence and contemporary experience show that all such security measures have some vulnerabilities which criminals are quick to identify and exploit. With time, all security, even sophisticated or well-designed solutions, will be defeated (especially if the reward of success provides sufficient motivation). There is thus a perennial struggle between defenders and attackers to secure city space, infrastructures and systems that provide adequate protection but are not so restrictive that they seriously inconvenience users or inhibit essential economic urban functions.

Smart city technologies are no different, being afflicted with a range of security vulnerabilities and risks, and an ongoing struggle is now evident between the cybersecurity industry and criminals and variously motivated hackers. However, while the base motivations to break into these systems might remain timeless (e.g., theft, extortion, impersonation, vandalism, malicious disruption), the nature of their performance is different. Because smart city technologies rely on networked digital computation, exploits of their vulnerabilities can be undertaken at distance and attacks can be masked, reducing the risk of detection and capture for perpetrators. Moreover, the use of software tools to automate hacking has greatly lowered costs and "super empowered" individual actors to conduct virtual criminality against multiple targets simultaneously, potentially affecting thousands of systems in different cities. Unauthorized access is often made easier because the so-called "attack surfaces" – the set of ways that a system might be susceptible to a breach – are multiplied due to a system's many interlocking parts, which are owned and controlled by a diverse set of stakeholders, making it difficult to secure every aspect of a large infrastructure or utility network. The rewards for success can also be significant, for example in the case of a data breach providing access to millions of user details, or in the case of vandalism/terrorism shutting down the entire electricity supply to a city, and can garner large amounts of publicity.

The nature of cyberattacks

Cyberattacks seek to "alter, disrupt, deceive, degrade, or destroy computer systems and networks or the information and/or programs resident in or transiting these systems or networks" (Owens et al., 2009: 1). There are three distinct forms of cyberattack against operational systems: *availability attacks* that seek to close a system down or deny service use; *confidentiality attacks* that seek to extract information and monitor activity; and *integrity attacks* that seek to enter a system to alter information and settings (and plant malware and viruses) without being noticed by the legitimate operator/owner (Singer and Friedman, 2014).

Cyberattacks can be performed by multiple different actors, from nation-state intelligence agencies and militaries, terrorist groups, organized criminals, hacker collectives, political and socially motivated activists, to "lone wolf" hackers, "script kiddies" and bored teenagers. It is estimated that over 100 nations have government funded and directed cyberattack units, many capable of targeting critical urban infrastructure (Goodman, 2015). Anecdotal evidence from media reporting indicates a significant increase in organized criminals conducting thefts and frauds by targeting online systems, including so-called "ransomware" attacks that are a virtualized means of monetary extortion against organizations (Hern, 2016).

Cyberattacks try to exploit one of five major vulnerabilities of digital technologies that are central to smart city systems.

Weak software security and data encryption: Research has detailed that, on average, there are 30 errors or possibly exploitable bugs for every 1,000 lines of code (Li et al., 2004). In typical large systems being deployed in cities there are millions of lines of code that produce hundreds of potential zero-day exploits (as yet unknown security vulnerabilities) for network viruses, malware, and directed hacks. Moreover, research by cybersecurity specialists has revealed that many smart city systems have been constructed with no or minimal security (such as no user authentication, or using default or weak passwords, e.g., "admin", "1234") (Cerrudo, 2015). Further, city governments and vendors of smart city technologies too often deploy them without undertaking thorough cybersecurity testing and where encryption is used, security issues can arise regarding how it is operated (Cerrudo, 2015).

Use of insecure legacy systems and poor ongoing maintenance: Many smart city technologies are layered onto much older infrastructure that relies on software and technology created 20 or 30 years ago, which has not been upgraded for some time, nor can they be migrated to newer, more secure systems (Rainie et al., 2014; Cerrudo, 2015). These technologies can create inherent vulnerabilities to newer systems by providing so-called "forever-day exploits" (holes in legacy software products that vendors no longer support and thus will never be patched). Even in the case of newer technologies, it can be difficult to test and rollout patches onto critical operational systems that need to be always on (Cerrudo, 2015).

System interdependencies and large and complex attack surfaces: The complexity of smart city systems means that it can be difficult to know which components are exposed and in what ways, to measure and mitigate risks, and to ensure end-to-end security (Cerrudo, 2015). Even if independent systems are secure, linking them to other systems can potentially open them to risk, with the level of security only guaranteed by the weakest link. Moreover, the interdependencies between technologies and systems mean that they are harder to maintain and upgrade. Beyond being hacked, the complexity of systems also increases the chances of "normal accidents" (e.g., programming bugs, human errors) that cause unanticipated failures (Perrow, 1984; Townsend, 2013).

Cascade effects: The interdependencies between smart city technologies and systems have the potential to create cascade effects, with failures or disruption

having knock-on impacts that result in the failure of other critical utilities or services (cf. Little, 2010). For example, a cyberattack on telecommunications infrastructure could cascade into an urban operating system that then cascades into the other systems, such as traffic management or emergency response. This is one of the key security risks of an urban operating system, wherein several systems are linked together to enable a "system of systems" approach to managing city services and infrastructures thus undoing the mitigating effects of using a siloed approach (i.e., fully separate system with physically independent telecommunications cabling and sources of power, etc.) (Little, 2010). A successful cyberattack on the electricity grid has huge cascade effects as it underpins so many activities such as powering homes, workplaces, and a plethora of other essential infrastructures. For example, a sophisticated cyberattack on the software controlling parts of Ukraine's electricity grid switched off the power to about a quarter of a million consumers for several hours in December 2015 (Zetter, 2016).

Human error and deliberate malfeasance of disgruntled (ex)employees: Technical exploits can be significantly aided by human error, for example, employees responding to phishing emails and installing viruses or malware, or naively inserting infected datasticks into computers (Singer and Friedman, 2014). In some cases, there are weaknesses in software system designs, such that they can be easily and surreptitiously sabotaged by disgruntled present and ex-employees.

These vulnerabilities are exacerbated by a number of factors, not least that it is often unclear who is responsible for maintaining security across complex systems and infrastructures when several companies and stakeholders collaborate in their design, supply hardware and software, and operate and use various elements (US DHS, 2016). This is exacerbated with respect to urban management, where city administrations are under increasing pressure for year-on-year "efficiency" savings that leads to an under-investment in infrastructure and its security maintenance, an over-reliance on legacy systems, outsourcing that minimizes in-house knowledge, and difficulties in recruiting and retaining skilled IT staff. With respect to the latter, there is a lack of investment in dedicated cybersecurity personnel and leadership (in the form of Chief Information Officer or Chief Technology Officer) and Computer Emergency Response Teams (CERTs) in city governments (Cerrudo, 2015). Any cybersecurity plans cities do possess are often siloed with respect to particular systems and departments so that cross-function assessment and response is lacking (Cerrudo, 2015).

In addition, it is clear that many smart city vendors have little or no experience in embedding security features into their products – despite claims made in their marketing literature – and many systems possess significant vulnerabilities. These vendors can impede security research by limiting access to their systems for testing, thus enabling them to continue to release unsecured products without oversight or accountability (Cerrudo, 2015). Moreover, too many cities have been lax in insisting on strong security controls and response within the procurement process for new systems.

Risks to smart city infrastructure

There is a growing body of well documented, real-world examples of malicious cyber-attacks aimed at city infrastructures. Many of these are relatively inconsequential, such as randomly directed probes of connected computers and scans across publicly available Internet addresses, and are unsuccessful. However, a small number are much more significant and involve a security breach. Between 2010 and 2014, the US Department of Energy (that oversees the power grid, regulates power generation, and manages the nuclear weapons arsenal) documented 1,131 cyberattacks, of which 159 were successful (Reilly, 2015). In 53 cases, these attacks were "root compromises", meaning that the attackers gained administrative privileges to computer systems, stealing various kinds of personnel and operational information, and potentially doing other damage (Reilly, 2015). There have been a range of cyberattacks on transport management systems, as well as proof-of-concept demonstrations of possible attacks. While the idea of crippling a city by disrupting the flow of traffic by hacking its management is not new – for example, it was a central plot device in the 1969 heist movie, *The Italian Job* – it can now be done remotely and is harder to defend against. For example, a cyberattack on a key toll road in Haifa, Israel, closed it for eight hours causing major traffic disruption in 2013 (Hodson, 2014); (for details on widespread vulnerabilities in wireless-accessible traffic signals see Ghena et al., 2014). A ransomware attack on the San Francisco municipal rail network led to ticketing machines being removed from service for several days (Gibbs, 2016). A teenager in Lodz, Poland, managed to hack the city's tram switches, causing four trams to derail and injuring a number of passengers (Nanni, 2013). In the United States, air traffic control systems have been hacked and Federal Aviation Administration servers compromised, with malicious code installed onto control networks (Goodman, 2015). Vehicles are also open to being hacked given that new cars contain so many digital controls and sensors and are connected to wireless networks (Greenburg, 2015).

All essential urban services including the electricity grid, water supply, and road traffic control rely on Supervisory Control and Data Acquisition (SCADA) systems that are used to control functions and material flows. These systems measure how an infrastructure is performing in real-time and enable either automated or human operator interventions to change settings. Many deployments are from the 1980s onwards and some contain "forever-day" exploits. A number of SCADA systems have been compromised, with hackers altering how the infrastructure performs or causing a denial-of-service. The most infamous documented SCADA hack to date was the 2009 Stuxnet attack on Iran's uranium enrichment plant (Zetter, 2015).

Smart city technologies are linked together via a number of communications technologies and protocols such as Long Term Evolution (4G LTE), Global System for Mobile Communication (GSM), Code Division Multiple Access (CDMA), WiFi, bluetooth. All of the modes of networking and transferring data are known to have security issues that enable data to be intercepted by third parties and provide unauthorized access to devices. Some of these protocols are so complicated

that they are difficult to implement securely. Likewise, telecommunication switches that link together the local and long distance Internet infrastructure are known to have vulnerabilities, including manufacturer and operator back-door security access and access codes that are infrequently updated (Singh and Pelton, 2013).

Securing smart cities

Given the scale and diversity of security flaws in the smart city, and their growing number of cyberattacks, how can vulnerabilities in smart cities technologies be addressed to minimize risk? To date, the strategy adopted for securing the smart city has largely been the use of technical mitigation solutions, such as access controls, encryption, IT industry standards and security protocols, and software patching regimes, along with staff training. While this has had some effect, given the vital nature of smart city technologies and infrastructures to urban life, it has become obvious that securing such systems requires a wider set of systemic interventions that encompass mitigation (lessening the force or intensity of something occurring) and prevention (stopping something from happening or arising), and ensure enactment through both market-led initiatives and governance-led regulation and enforcement.

Conventional mitigation

The common approach to securing smart city systems has been to utilize well-known software security tactics to try and prevent access and to enable restoration if a compromise occurs – for example, the use of access controls (username/password, two-stage authentication, biometric identifiers), properly maintained firewalls, virus and malware checkers, end-to-end strong encryption, and procedures to ensure routine software patching and the ability to respond with urgent updates to close vulnerabilities as they occur, audit trails of usage and change logs, and effective offsite backups and emergency recovery plans. Where feasible, systems should have built-in redundancy to ensure that if the primary delivery of a critical system fails, a secondary system automatically takes its place. Such redundancy might include the use of decentralized cloud-based solutions or a completely separate technological solution. While an optimal solution, it is also the case that creating genuine redundancy is often difficult and expensive.

The extent to which the protections are available varies across technologies and vendors; and the application across different institutions and companies is also inconsistent. Moreover, in complex, distributed systems with many components these solutions need to work equally across the complete system since the whole infrastructure/enterprise is only as strong as the weakest link. Further, it is often the case that these kinds of solutions are layered on after a system has been developed rather than being integral to the design.

These technical solutions are often bolstered by a vigilant IT staff whose job it is to oversee the day-to-day maintenance of these systems, including monitoring

security issues and reacting swiftly to new cyberattacks and breaches. In addition, non IT-staff across an organization can be trained to maintain good practices with respect to security, such as adopting stronger passwords, routinely updating software, encrypting files, and avoiding phishing attacks. However, training is often conducted only once and ongoing staff compliance with best practice is hard to achieve.

While these security measures have genuine utility, they are far from a complete solution, particularly as smart technologies become ever more critical to the smooth functioning of cities. Instead, a more systemic approach needs to be adopted in relation to both technical design and training. In particular, a security-by-design approach that is proactive and preventative, rather than reactive and remedial, needs to be employed by city governments and key institutions responsible for urban management and infrastructure provision. Security-by-design seeks to build strong security measures into systems from the outset rather than attempting to layer them on after initial development. This requires security risk assessment to be a fundamental part of the design process and all aspects of security systems to be rigorously tested before the product is sold, including a pilot phase testing the security when deployed in real-world contexts and operating as part of a wider network of technologies (to ensure end-to-end security). It also means having in place an ongoing commitment to cybersecurity, including a mechanism to monitor products throughout their life cycle, a process of supporting and patching them over time, and a procedure for notifying customers when security risks are identified. With respect to existing city software systems and control infrastructure, all vendors should be asked for full security documentation and procedures, and a comprehensive testing of their security should be undertaken to identify weak points, undertake remedial security patching, and to upgrade future service level agreements with respect to enhanced security. This is especially the case for legacy systems. If systems cannot be remedially fixed and forever-day exploits remain that could bring down critical systems, then firm plans need to be put in place for upgrades or replacement. It should be noted that there are cost implications in mandating better security and this needs to be factored into smart city investment strategies.

With respect to overseeing the security aspects of smart city technologies a core security team is essential within urban administrations with specialist skills and responsibilities above and beyond day-to-day IT administration. The work of this team would include: undertaking threat and risk modelling; actively testing the security of smart city technologies (rather than simply monitoring and trusting vendor reassurances); conducting ongoing security assessments; preparing and reviewing detailed plans of action for different kinds of cybersecurity incidents; liaising with the city departments and companies administering smart city initiatives; and coordinating staff training on security issues. The staff would also constitute a city's Computer Emergency Response Team to actively tackle any on-going cybersecurity incidents (Cerrudo, 2015). As a routine part of their work, the core security team should consult with cybersecurity vendors to stay up-to-date on potential

threats and solutions (Nanni, 2013). In addition, the team creates a formal channel for security feedback and ethical disclosure, enabling bugs and security weaknesses to be reported by members of the consultants, academics, and allied technology companies. Initial security assessments would be carried out as early as possible, for example in the scoping and procurement phases of technological adoption, to ensure the solutions developed conform to expectations. Part of any assessment should be a consideration of whether systems should be kept in siloes to limit cascade effects. Given cost constraints and lack of strategic foresight, very few cities presently have core cybersecurity teams and are therefore underprepared to deal with a serious cyberattack.

Enactment and enforcement

While it is one thing to advocate for stronger mitigation measures, it is another to ensure that a more systemic approach to cybersecurity for smart cities is widely implemented and enforced. More attention needs to be paid to the mechanisms to incentivize participation by both the public and commercial sector, and to penalize those who fail to improve security of their products, systems, and services. There are two routes to improving mitigation measures: market-led adoption and government-led regulation and legal enforcement.

The market-led approach consists of commercial vendors developing smart city technologies taking a proactive, self-regulatory stance to security. Here, software companies choose to adopt security-by-design as a de facto standard, collaborate with each other to create effective industry-wide standards, and establish best practices. They ensure security across complex, interdependent systems, and work more closely with the rapidly growing cybersecurity industry in order to improve their products. In so doing, security becomes an expected norm and the adoption of a serious approach to security by companies provides competitive advantage over those that do not comply. In part, the market-led approach is driven by competition; fear of reputational damage and litigation caused by a major security scandal; and the benefits of self-regulation, rather than the approach of statutory enforcement with legal prosecution and fines.

While a market-led approach to security does presently exist, it predominantly adopts the weak mitigation approach detailed above and not security-by-design. In part this is because there has been weak pressure from buyers for enhanced security, mainly due to a poor understanding of security vulnerabilities and their potential consequences and inadequate procurement practices. Moreover, the imperatives to get product to market as quickly as possible (often to pre-empt a competitor) and turn a profit mean that security corners are being cut. As such, market-led responses will need to be accompanied by more "top-down" regulation and better management practices by city authorities and utility operators.

The regulation and management-led approach seeks to encourage secure deployment of smart city technologies through compliance measures and active oversight. The former requires the formulation of security standards, directives, and

best practices that smart city deployments must comply with or face some form of penalty, such as prosecution, fines, or loss of contract. There are now a host of smart city standards initiatives underway – by bodies such as the International Standards Organization, British Standards Institute, American National Standards Institute, and City Protocol – aimed at defining minimum specifications for technical development and deployment of core technologies. The latter necessitates setting up management structures and procedures for ensuring compliance is being met and enforced. In addition, city administrations must call for security-by-design and integral life-long security maintenance (including on-time patching and 24/7 incident response) into the procurement process and subsequent service level contracts. They should also support whistle-blowers who wish to expose security vulnerabilities and require the public reporting of security breaches.

A preventative approach

Even with a strong mitigation strategy and effective enforcement procedures, it is not possible to eradicate all the security vulnerabilities and associated risks from the smart city. There is, therefore, a case to be made for considering a preventative approach, one that involves building some urban infrastructure and control systems that are deliberately "deaf" (not networked and remotely accessible) and "dumb" (i.e., not automated by code), which would elide many software security overheads. A preventative approach is quite straightforward to articulate – simply put, "do not adopt smart city technologies as presently conceived"; the best way to prevent risks from materializing is not to create vulnerabilities in the first place.

Yet making the case for such an approach is much more difficult in practice because of the perceived benefits of creating a smart city. Such a cautious, preventative approach, that questions seriously the commercial logics and profit streams of many hardware vendors and software developers, will be derided as "backward looking" and having a neo-Luddite mentality (see Jones, 2013). Advocating a preventative approach is considered a radical means of securing smart cities as it requires a reframing of the value around technology in regards to convenience/efficiency and security/safety. It requires a counter-narrative against "smarter is better" and advocacy for conventional electro-mechanical components and systems that run reliably without additional software monitoring and network access.

There is a case, however, to be made that the greater potential risks networked infrastructure poses, plus the higher cybersecurity overheads, outweigh the efficiency and functionality gains promised. In the era of ubiquitous wireless connectivity, cloud-computing and remote control, the notion of having so-called "air-gapped" systems might seem counter-intuitive. However, it can be an effective method of security that prevents hacking and cascade effects and significantly reduces vulnerabilities.

Equally, there are reasons to be sceptical of the benefits claimed by advocates (who are often self-interested) for new cyber-physical systems as it is well noted

that they tend to oversell the promises of smart city technologies while ignoring their threats. Many existing smart city system deployments have not delivered the anticipated gains in efficiency, flexibility, productivity and convenience. In regards to the IoT, presently there is little perceivable gain or real benefits to the functioning and management of cities in many sensor-net deployments (though they benefit vendors through their sale/servicing and potential monetization of data streams). In fact, if anything, some newly software-enabled systems make routine tasks more complex to complete, error-prone, unreliable, stressful, costly in time and cognitive attention, and less secure, as well as raising issues with respect to excessive surveillance and personal privacy (Greenfield, 2013; Kitchin, 2016). In other words, networking city infrastructure and introducing new systems do not necessarily improve performance, yet they do make them more vulnerable to cyberattacks.

Nonetheless, at present, implementing preventative measures will be difficult to promote and promulgate given the widespread adoption of techno-utopian discourses of "progress" enacted by smart urbanism. This is especially the case in the current neoliberal climate that encourages cities to form public-private partnerships with companies and to outsource or privatize services, and where access to government grants will be difficult without claiming to create and implement innovative and cutting-edge smart city solutions. This may change though if the "cutting-edge" of city management becomes recognized as the "bleeding-edge" of cyber insecurity.

Conclusion

This chapter has examined issues around the security of smart cities. In an ironic twist, smart city technologies are promoted as an effective way to counter and manage uncertainty and risk, yet they paradoxically induce new risks, including making city infrastructure and services more vulnerable and open to extensive forms of digital vandalism, network disruption and cyber-criminal exploitation. This paradox has largely been ignored by commercial and governmental interests or tackled through conventional mitigation approaches. While the majority of cyberattacks are presently being repulsed by software tools and management practices there is real potential for much more disruptive and damaging impacts on critical systems. Criminals and other actors are developing more sophisticated methods of hacking, and security measures fail to keep pace. It may be that more severe disruption of critical infrastructure has so far been avoided because nation-state actors do not want to reveal their capabilities and they fear retaliation from adversaries (Rainie et al., 2014).

Present strategies for addressing the vulnerabilities and risks posed by the mass adoption of networked technologies for city management are inadequate and predominantly rely on existing technical and training mitigation strategies and market-led solutions. Instead, there needs to be a widening and deepening of mitigation strategies to include security-by-design as a de facto approach for all future smart

city procurement, a comprehensive assessment of existing urban infrastructures and information systems and remedial security patching or replacement, the formation of core security and computer emergency response teams within city administrations with specialist skills. This should be complemented by a management and regulation approach to smart city technologies and implementation, rather than simply a market-led approach, to ensure active oversight and compliance with security standards, best practices, municipal policy, and third-party service contracts. Moreover, serious consideration should be given to a preventative approach to security, wherein critical infrastructure is air-gapped or not given the "smart" treatment when it is not really needed.

It is not feasible to halt the smart city agenda, and much of the adoption of networked technologies and software systems by municipal authorities across the world cannot simply be removed. However, it is not too late to recognize the extent of the new cybersecurity vulnerabilities and risks posed by these technologies and to put in place strategies and approaches to mitigate and prevent them.

Acknowledgements

This chapter is a modified version of Kitchin, R. and Dodge, M. 2017. "The (in) security of the smart cities: vulnerabilities, risks, mitigation and prevention", *Journal of Urban Technology*. Rob Kitchin's contribution is based on research funded by a European Research Council Advanced Investigator grant, The Programmable City (ERC-2012-AdG-323636).

References

Cerrudo, C. 2015. "An emerging US (and world) threat: cities wide open to cyber attacks", *Securing Smart Cities*http://securingsmartcities.org/wp-content/uploads/2015/05/CitiesWideOpenToCyberAttacks.pdf.

Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J. and Halderman, J.A. 2014. "Green lights forever: analyzing the security of traffic infrastructure", *Proceedings of the 8th USENIX Workshop on Offensive Technologies*www.usenix.org/system/files/conference/woot14/woot14-ghena.pdf

Gibbs, S. 2016. "Ransomware attack on San Francisco public transit gives everyone a free ride", *Guardian*, 28 November.http://www.theguardian.com/technology/2016/nov/28/passengersfree-ride-san-francisco-muni-ransomeware (accessed 5 October 2017).

Goodman, M. 2015. *Future Crimes*. New York: Bantam Press.

Greenburg, A. 2015. "Hackers remotely kill a Jeep on the highway, with me in it", *Wired*, 21 July.http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway (accessed 5 October 2017).

Greenfield, A. 2013. *Against the Smart City*. New York: Do Press.

Hern, A. 2016. "Ransomware threat on the rise", *Guardian*, 3 August, http://www.theguardian.com/technology/2016/aug/03/ransomware-threat-on-the-rise-as-40-of-businesses-attacked (accessed 5 October 2017).

Hodson, H. 2014. "Gridlock alert", *New Sci*, 9 August, https://www.sciencedirect.com/science/article/pii/S0262407914615323 (accessed 30 May 2018).

Jones, S.E. 2013. *Against Technology: From the Luddites to Neo-Luddism*. London: Routledge.

Kitchin, R. 2016. "The ethics of smart cities and urban science", *Philosophical Transactions A*, 374(2083): 1–15.

Kitchin, R. and Dodge, M. 2017. Online first. "The (in)security of the smart cities: vulnerabilities, risks, mitigation and prevention", *Journal of Urban Technology*, https://www.tandfonline.com/doi/abs/10.1080/10630732.2017.1408002.

Li, P.L., Shaw, M., Herbsleb, J., Ray, B. and Santhanam, P. 2004. "Empirical evaluation of defect projection models for widely-deployed production software systems", *ACM SIGSOFT Software Engineering Notes*, 29(6): 263–272.

Little, R.G. 2010. "Managing the risk of cascading failure in complex urban infrastructures", in Graham, S. (ed.), *Disrupted Cities: When Infrastructure Fails*. London: Routledge, pp. 27–39.

Nanni, G. 2013. *Transformational "Smart Cities": Cyber Security and Resilience*. Mountain View, CA: Symantec.

Owens, W.A., Dam, K.W. and Lin, H.S. 2009. *Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities*. Committee on Offensive Information Warfare; National Research Council. Washington DC: National Academic Press.

Perrow, B. 1984. *Normal Accidents: Living With High-Risk Technologies*. New York: Basic Books.

Rainie, L., Anders, J. and Connolly, J. 2014. "Cyber Attacks Likely to Increase", Digital Life in 2025. Pew Research Center. http://www.pewinternet.org/files/2014/10/PI_FutureofCyberattacks_102914_pdf.pdf. (accessed 5 October 2017).

Reilly, S. 2015. "Records: Energy Department Struck by Cyber Attacks", CNBC, 10 September.http://www.cnbc.com/2015/09/10/records-energy-department-struck-by-cyber-attacks.html (accessed 5 October 2017).

Singer, P.W. and Friedman, A. 2014. *Cybersecurity and Cyberwar*. Oxford: Oxford University Press.

Singh, I.B. and Pelton, J.N. 2013. "Securing the cyber city of the future", *The Futurist*, 47(6): 22.

Townsend, A.M. 2013. *Smart Cities: Big Data, Civic Hackers and the Quest for a New Utopia*. New York: Norton.

US DHS. 2016. *Strategic Principles for Securing the Internet of Things*, 15 Novemberhttp://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016–1115-FINAL.pdf (accessed 5 October 2017).

White, J.M. 2016. "Anticipatory logics of the smart city's global imaginary", *Urban Geography*, 37(4): 572–589.

Zetter, K. 2015. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Broadway Books.

Zetter, K. 2016. "Inside the cunning, unprecedented hack of Ukraine's power grid", *Wired News*, 3 March, http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid (accessed 5 October 2017).