The (in)security of smart cities: vulnerabilities, risks, mitigation and prevention

Rob Kitchin[1] and Martin Dodge[2]

1. NIRSA, National University of Ireland Maynooth, rob.kitchin@nuim.ie
2. Department of Geography, University of Manchester, m.dodge@manchester.ac.uk

The Programmable City Working Paper 24

http://progcity.maynoothuniversity.ie/

13 February 2017

Published as an open access pre-print on SocArXiv: https://osf.io/preprints/socarxiv/f6z63

Abstract

In this paper we examine the current state of play with regards to the security of smart city initiatives. Smart city technologies are promoted as an effective way to counter and manage uncertainty and urban risks through the effective and efficient delivery of services, yet paradoxically they create new vulnerabilities and threats, including making city infrastructure and services insecure, brittle, and open to extended forms of criminal activity. This paradox has largely been ignored or underestimated by commercial and governmental interests or tackled through a technically-mediated mitigation approach. We identify five forms of vulnerabilities with respect to smart city technologies, detail the present extent of cyberattacks on networked infrastructure and services, and present a number of illustrative examples. We then adopt a normative approach to explore existing mitigation strategies, suggesting a wider set of systemic interventions (including security-by-design, remedial security patching and replacement, formation of core security and computer emergency response teams, a change in procurement procedures, and continuing professional development). We discuss how this approach might be enacted and enforced through market-led and regulation/management measures, and examine a more radical preventative approach to security.

Keywords: crime, cyberattacks, mitigation, risk, security, smart cities, urban resilience

Introduction

Over the past two decades there has been a concerted move to network urban infrastructures to utilise computation to try and solve urban problems and deliver city services more efficiently. Such endeavours are now encapsulated within the notion of smart cities, a world-wide movement that seeks to transform urban governance, management and living through the use of new networked digital technologies. For advocates, the creation of smart cities will help address issues of urban resilience and sustainability in a time of rapidly increasing population, environmental change, and fiscal austerity (see Söderström *et al.*, 2014; 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 systems, communication services), a number of commentators have noted that they also create a paradoxical situation wherein the promised benefits (such as convenience, economic prosperity, safety, sustainability) are accompanied by unintended consequences and new variances of traditional problems (e.g., reproducing inequality, creating security and criminal risks, environmental externalities) (see Datta 2015; Greenfield, 2013; Singh & Pelton, 2013; Townsend, 2013). 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.

In contrast, in this paper we examine this paradoxical relationship in depth, detailing how smart city technologies designed to produce urban resilience and reduce risks are actually opening up the urban systems they are meant to augment to new forms of vulnerability and risk. In particular, we are interested in considering 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, computer glitches, network viruses, hacks and criminal and terrorist enterprise (Little, 2010 Kitchin & Dodge, 2011; Townsend, 2013; Cerrudo, 2015). We are especially interested in security vulnerabilities and the extent to which it is becoming possible to hack and disrupt smart city technologies and to commit new variances of criminal activity.

As the burgeoning literature on crime and the city details, for as long as there have been urban societies there has been criminal activity and attempts to penetrate, attack, defraud and disrupt city infrastructure and public services (Evans and Herbert, 1989; LeBeau & Leitner, 2011; Hall, 2012). Attempts to limit and defend against such crimes have become

built into the fabric of cities themselves through architecturally-enacted defences, strong doors, locks, window grills, high walls and fences, security alarms, and CCTV (Manaugh, 2016). However, history has shown that all these security measures have some vulnerabilities that 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 systems that provide adequate protection but are not so restrictive that they seriously inconvenience users or inhibit essential economic transactions.

Smart city technologies are no different being afflicted with a range of security vulnerabilities and risks and an on-going 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, impersonation, vandalism, malicious attack; see Schneier, 2003), 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 impacting many different cities. Unauthorised access is often made easier because the so-called 'attack surfaces' – the set of ways that a system might be susceptible to an attack (Bellovin, 2016) - 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 (Article 29 DPWP, 2014; Cerrudo, 2015; Durbin, 2015). 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.

In the first part of the paper we detail the various security vulnerabilities of smart cities and their associated risks, providing contemporary illustrative examples from European and North American cities. In second part we chart the ways in which these vulnerabilities and risks are being tackled through mitigation strategies, how these strategies might be further encouraged and complemented by market-based and governance-based incentives and regulation, and consider a more radical preventative strategy. Our approach is *normative*. Rather than providing another critique of the smart city, this time by charting the paradoxical situation in which technologies designed to tackle urban problems are introducing new

vulnerabilities and risks, or seeking to frame such risks within the discourses of the risk society (Beck, 1992) or urban resilience (Mackinnon & Derickson, 2013), we are more interested in examining the security challenges and threats faced by cities today and over the coming decade and how they might be more effectively mitigated and prevented. Our approach is guided by a recognition that the use of software systems and networked technologies to manage and govern cities is firmly established and is only likely to become more entrenched, and the need for a coherent approach to security that extends beyond technical solutions.

Security vulnerabilities and risks of smart cities

There are two key security risks with respect to the emergence of smart cities. The first is the security of newly installed 'intelligent' technologies and 'smart' upgrades to existing infrastructures and systems and the extent to which these are vulnerable to being hacked. The second is the security of the data generated, stored and shared across such technologies and infrastructures. The latter is directly related to the former as improper access to data is often achieved via security weaknesses in a system's components, architecture and operation. In this sense, information security (data protection) has converged with operational security (making sure things work reliably and with integrity). Here, we are most interested in the vulnerabilities of city infrastructures and systems rather than data security per se; that is, the extent to which their operation can be compromised and functioning disrupted.

The principal means of compromising a smart city technology is through cyberattacks that 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 (such as changing settings so that components exceed normal performance, erasing critical software, planting malware and viruses) (Singer & Friedman, 2014). Cyberattacks can be performed by multiple different actors, from nation state intelligence agencies and militaries, terrorist groups, organised criminals, hacker collectives, political and socially motivated activists to 'lone wolf' hackers, 'script kiddies'

and bored teenagers[1]. Former FBI Director, Robert Mueller, has claimed that 108 nations have government funded and directed cyberattack units, targeting critical infrastructure and industrial secrets (Goodman, 2015). Anecdotal evidence from media reporting indicates a significant ramping up of organised criminals conducting thefts and frauds by targeting online systems, including spate of so-called 'randomware' attacks against organisations (Hern, 2016).

In general, cyberattacks seek to exploit one of five major vulnerabilities of digital technologies that are central to smart city systems. The first of these is *weak software security and data encryption*. Research by a Carnegie Mellon University team in 2004 detailed that, on average, there are 30 errors or possibly exploitable bugs for every 1000 lines of code (Li *et al.*, 2004). In typical large systems being deployed in cities there are millions of lines of code that produces thousands of potential zero-day exploits (as yet unknown security vulnerabilities) for network viruses, malware and directed hacks. Research by cybersecurity specialists has detailed how many smart city systems have been constructed with no or minimal security (Cerrudo, 2015). For example, using the *Shodan* search engine (www.shodan.io see Bodenheim *et al.*, 2014) it is possible to find all kinds of devices and control systems connected to the internet – from networked thermostats for heating systems to traffic control systems and command-and-control centres for nuclear power plants – many of which have been found to have little to no security (such as no user authenication, or using default or weak passwords, e.g., 'admin', '1234'). Moreover, city governments and vendors of smart city technologies often deploy them without undertaking cybersecurity testing (Cerrudo, 2015). In the case of some 'Internet of Things' (IoT)[2] deployments, it can be difficult to ensure end-to-end security because most sensors and low-powered devices on the market do not have sufficient computing power to support an encrypted network link (Article 29 DPWP, 2014). Where encryption is used, security issues can arise due to how it is operated (Cerrudo, 2015).

The second area of vulnerability is due to the *use of insecure legacy systems and poor 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

[1] Computer hacking culture has a long history and with diverse and contested meanings (Levy, 1984), but the term has come typically to be applied to those with malicious or criminal intent.

[2] The IoT is a fast developing set of identification and technologies that connect together formally 'dumb' physical objects and make them addressable through the internet and potential facilitate all manner of new activities and processes in relation to these objects, often in highly automated and autonomous fashion. As such IoT is critical element in creation of what Dodge and Kitchin (2005) called the 'machine-readable world'.

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) (Townsend, 2013). Even in the case of newer technologies, it can be difficult to test and rollout patches onto critical operational systems that need to always be on (Cerrudo, 2015).

The third vulnerability is that smart city systems are typically large, complex and diverse, with *many interdependencies and large and complex attack surfaces.* Such complexity means it can be difficult to know what and how all the components are exposed, to measure and mitigate risks, and to ensure end-to-end security (Article 29 DPWP, 2014; Cerrudo, 2015; Durbin, 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 (Sarma, 2015). 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).

The interdependencies between smart city technologies and systems have the potential to create *cascade effects*, wherein 'highly interconnected entities rapidly transmit adverse consequences to each other' (Durbin, 2015, no pagination; see also Little, 2010). For example, a cyberattack on an electrical power infrastructure could cascade into an urban operating system that then cascades into the other systems such as traffic management, emergency services, and water services. Indeed, this is one of the key security and resilience 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 cabling and sources of power, etc.) (Little, 2011). A successful cyberattack on the electricity grid has huge cascade effects as it underpins so many activities such as powering homes, workplace, and a plethora of other essential infrastructure, and so on. 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).

Finally, there are multiple vulnerabilities arising from *human error and deliberate malfeasance of disgruntled (ex)employees.* Technical exploits can be significantly aided by human error, for example, employees opening phishing emails and installing viruses or

malware, or naively inserting infected datasticks into computers (Singer and Friedman, 2014). In other cases, appropriate security software is not installed or is configured incorrectly, or manufacturer installed codes are not changed or system security is not kept up-to-date (Cerrudo, 2015). There are weaknesses in software system designs such that they can be easily and surreptitiously sabotaged by disgruntled present and ex-employees. For example, Goodman (2015) details a case where an ex-employee altered the database records of a vehicle retailer who were using GPS trackers and remote control boxes to re-possess cars, randomly disabling cars and setting off their alarms. In addition, criminal hackers are adept at social exploits on trusted employees such as using phishing to release key information (e.g., usernames and passwords) that facilitate access. There is also evidence from the Snowden revelations that 'insiders' have been planted by State intelligence agencies with view to deliberately compromising the design of networking hardware and fundamental system parameters to facilitate electronic espionage, sabotage and cyber-warfare (Greenwald, 2014).

These vulnerabilities are exacerbated by a number of factors in relation to urban management. Cities and local council are under increasing pressure for year-on-year 'efficiency' savings. This affects security in three ways. First, there is long-term under-investment in infrastructure maintenance and an over-reliance on legacy systems. Second, depression of salaries in most public sector organisations make it more difficult to recruit and retain skilled and motivated IT staff to properly implement and maintain smart city technologies. Crucial IT maintenance increasingly uses self-employed contractors and outsourced services, on the one hand deskilling core capacities and eroding institutional memory in the public sector, and on the other creating distributed accountability with a fractured set of bodies (with contracted services, service-level agreements, multi-agencies teams, remote helpdesks) overseeing security, which often leads to a lack of continuity, coordination and responsibility. Third, 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). Cybersecurity expertise is usually limited to a handful of personnel and training across the wider workforce is limited or non-existent (increasing the likelihood of human error). 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 (Cerrudo, 2015; Lomas, 2015). Furthermore, these vendors can impede security research by limiting access to their systems for testing, enabling them to continue to release unsecured products without oversight or accountability (Cerrudo, 2015). Further, too many cities have been lax in insisting on strong security controls and response within the procurement process for new systems.

Collectively, security vulnerabilities mean that cyberattacks on important urban infrastructure and city management systems have been increasing with implications for human safety and security. In 2016, the Chief Information Security Officer for the City of San Diego government reported that their systems were being hit by an average of 60,000 cyberattacks a day (Anand, 2016). The operators of the electricity supply grid in the United States report being under near constant cyberattack, with one utility recording that it was the target of approximately 10,000 cyberattacks each month (Markey and Waxman, 2013). Indeed, all five Commissioners of the Federal Energy Regulatory Commission agree that sustained and persistent cyberattacks against the digital infrastructure controlling the supply grid is the most serious threat to electricity reliability in American metropolitan areas (Markey and Waxman, 2013). Likewise, the Israel Electric Corp. reports that its servers register about 6,000 unique computer attacks every second, with other critical infrastructure also under continuous attempts to gain access (Paganini, 2013). Many of these cyberattacks 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, regulate power generation, as well as managing 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). In a 2014 study of nearly 600 utility, oil and gas, and manufacturing companies, about 70% reported at least one security breach that led to the loss of confidential information or disruption of operations in the previous 12 months (Prince, 2014); 78% expected a successful attack on their ICS (industrial control systems) or SCADA (supervisory control and data acquisition) systems in the next two years (Prince, 2014). The trends in data and opinions of informed commentators is that frequency, volume and severity of cyberattacks is only going

to increase. Moreover, it is evident that sophistication of attacks is outpacing the quality and depth of defences.

Similarly, there have been a number of cyberattacks on transport management systems in recent years, as well as proof-of-concept demonstrations of possible attacks. While the idea of crippling a city by disrupting the flow of traffic through computerised infrastructure is not new – for example, it was a central plot device in the 1969 heist movie, *The Italian Job* – but 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 (Paganini, 2013). A ransomware attack on the San Francisco municipal rail network led to ticketing machines being removed from service for two days (Gibbs, 2016). A research team from the University of Michigan managed to hack and manipulate more than a thousand wireless-accessible traffic signals in one city using a laptop, custom-software and a directional radio transmitter (Ghena *et al.*, 2014). Likewise, security consultants IOActive Labs have hacked traffic control sensors widely used around the world and altered traffic light sequencing and interactive speed and road signs (Cerrudo, 2014). A teenager in Lodz, Poland, managed to hack the city tram switches, causing four trams to derail and injuring a number of passengers (Nanni, 2013; Goodman, 2015). In the US, air traffic control systems have been hacked, Federal Aviation Administration servers compromised, and malicious code installed onto control networks, and the personal information of 58,000 workers stolen (Goodman, 2015). Vehicles are also open to being hacked given that a new car contains up to 200 sensors connected to around 40 electronic control units and can connect to wireless networks (Greenburg, 2015).

Every type of smart city solution and particular system components, including SCADA (supervisory control and data acquisition) systems, the sensors and microcontrollers of the Internet of Things, and network routers and telecommunication switches, are open to various forms of cyberattack. All essential urban services including the electricity grid, water supply, and road traffic control rely on 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. The implementation of SCADA systems can be traced back to the 1920s, but were extensively rolled out in the 1980s. As a consequence, many deployments are quite dated and contain

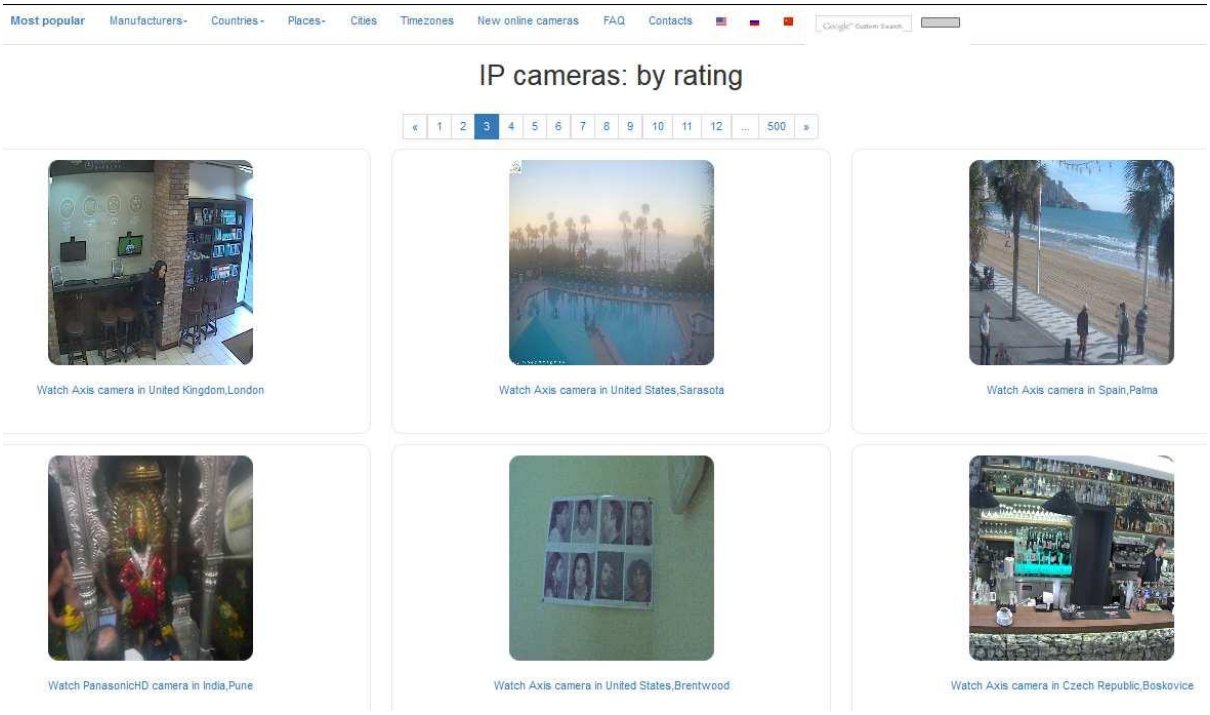
'forever-day' exploits[3]. A number of SCADA systems have been compromised, with hackers altering how the infrastructure performs, or causing a denial-of-service, or have stolen data. The most infamous SCADA hack to date was the 2009 Stuxnet attack on Iran's uranium enrichment plant in which the system was infected by malware that destroyed a number of centrifuges by running them beyond their design specifications. By 2010 over 90,000 Stuxnet infections were reported in 115 countries (Zetter, 2015).

The Internet of Things (IoT) refers to the connecting together of machine-readable, uniquely identifiable objects through the Internet such that they can communicate largely autonomously and automatically. Some objects are passive and can simply be scanned or sensed (such as smart cards with embedded RFID chips[4] used to access buildings and transport systems). Others are more active and include microcontrollers and actuators. All kinds of objects that used to be 'dumb', such as thermostats, domestic appliances security cameras, lighting systems (where the individual bulbs are addressable) are now becoming networked and 'smart', generating information about their use and becoming controllable from a distance. The security of the Internet of Things is highly variable, with some systems lacking encryption or usernames and passwords, and others open to infection by malware and firmware modification. The complex interdependencies of IoT mean that it has a large attack surface and multiple vulnerabilities (see Table 1). Demonstrating the scale of IoT vulnerability, one provocative project, Insecam.org provides access to the feeds of thousands of unsecured secured cameras available on the public internet from cities across the world (Cox, 2014) (see Figure 1). These cameras can also be turned off, with some lacking the function to be restarted remotely (Cerrudo, 2015). Others researchers have shown how to hack into smart lighting and take over control, with potentially serious consequences for personal safety (Chacos, 2016). In addition, IoT infrastructure can be used to perform other kinds of hacks, as with the Dyn denial of service attacks in autumn of 2016 in which many significant websites were disrupted by the Mirai botnet that took over unsecured IoT devices and used them to bombard Dyn servers (Woolf, 2016).

[3] This is a publicly known code error in a software product that the vendor is not able to or is not intending to fix, consequently there is no means of patching the software.

[4] These comprise a small physical electronic circuit and antenna that can be fix to physical objects and automatically broadcast a globally unique identification code number when queried by appropriate radio signal, see Frith, 2015.

Figure 1. A demonstration of global cybersecurity issues in terms of open security video feeds and webcams on the Internet. (Source: Authors' screenshot of insecam.org)



Smart city technologies are linked together via a number of communications technologies and protocols such as 4G LTE (Long Term Evolution), GSM (Global System for Mobile communication), CDMA (Code Division Multiple Access), WiFi, bluetooth, , NFC (Near-Field Communication), ZigBee (open wireless standard), and Z-Wave (wireless communication). Each 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 unauthorised access to devices. Some of these protocols are so complicated that they have 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 & Pelton, 2013). In addition, due to 'oversubscribing', wherein wireless carriers want to maximize use of spectrum licenses, networks only have capacity for a fraction of subscribers meaning that during a crisis when demand surges the system cannot cope, failing to connect both people and things (Townsend, 2013).

Table 1: The dimensions of risk with Internet of Things technologies related to the multiple attack surfaces and scale of potentially vulnerabilities exposed

Attack Surface	Vulnerability	Attack Surface	Vulnerability
Ecosystem Access Control	Implicit trust between components Enrolment security Decommissioning system Lost access procedures	***Local Data Storage***	Unencrypted data Data encrypted with discovered keys Lack of data integrity checks
Device Memory	Cleartext usernames Cleartext passwords Third-party credentials Encryption keys	***Third-party Backend APIs***	Unencrypted PII sent Encrypted PII sent Device information leaked Location leaked
Device Physical Interfaces	Firmware extraction User command line interface Administrative command line interface Privilege escalation Reset to insecure state Removal of storage media	***Vendor Backend APIs***	Inherent trust of cloud or mobile application Weak authentication Weak access controls Injection attacks
Device Web Interface	SQL injection Cross-site scripting Cross-site Request Forgery Username enumeration Weak passwords Account lockout Known default credentials	***Update Mechanism***	Update sent without encryption Updates not signed Update location writable Update verification Malicious update Missing update mechanism No manual update mechanism
Device Firmware	Hardcoded credentials Sensitive information disclosure Sensitive URL disclosure Encryption keys Firmware version display and/or last update date	***Ecosystem Communication***	Health checks Heartbeats Ecosystem commands Deprovisioning Pushing updates
Device Network Services	Information disclosure User command line interface Administrative command line interface Injection Denial of Service Unencrypted Services Poorly implemented encryption Test/Development Services Buffer Overflow UPnP Vulnerable UDP Services DoS	***Mobile Application***	Implicitly trusted by device or cloud Username enumeration Account lockout Known default credentials Weak passwords Insecure data storage Transport encryption Insecure password recovery mechanism Two-factor authentication
Administrative Interface	SQL injection Cross-site scripting Cross-site Request Forgery Username enumeration Weak passwords Account lockout Known default credentials Security/encryption options Logging options Two-factor authentication Inability to wipe device	***Cloud Web Interface***	SQL injection Cross-site scripting Cross-site Request Forgery Username enumeration Weak passwords Account lockout Known default credentials Transport encryption Insecure password recovery mechanism Two-factor authentication
Network Traffic	LAN		

	LAN to Internet Short range Non-standard		

Source: Adapted from Open Web Application Security Project, 2015. https://www.owasp.org/index.php/IoT_Attack_Surface_Areas (CC-BY)

Securing smart cities: mitigation and preventative

It is clear that smart city technologies currently being deployed have multiple vulnerabilities and that these will be exploited for various ends. A key question therefore concerns how such vulnerabilities can be addressed to minimize threats and risk? To date, the strategy adopted has largely been one of conventional, largely 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, we contend that the securing of smart cities is becoming of such significance to urban living that it 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 ensures enactment through both market-led initiatives and governance-led regulation and enforcement.

Conventional mitigation solutions

As noted, smart city technologies typically present large attack surfaces that expose a number of potential vulnerabilities, especially in control systems that contain legacy components using old software which has not been regularly patched. The typical approach to securing smart city systems has been to utilise a suite of well-known technical solutions and software security approaches 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 ability to respond with urgent updates to close exploits as they occur, audit trails of usage and change logs, and effective offsite backups and emergency recovery plans (see Table 2). Using these techniques, the aim is to reduce the attack surface as much as possible and to make the surface that is visible as robust and resilient as possible; and quickly recoverable in case of failure. However, the extent to which this suite of protections is 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 'baked-into' the design.

These technical solutions are often bolstered by 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 changing default and 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 not monitored.

Table 2: Standard technical aspects of software system security

Access	**Updating**	**Functionality**	**Design**
Effective end-to-end encryption on all communications	Up-to-date virus and malware checkers	Disabling unnecessary functionality	Isolating trusted resources from non-trusted
Enforce strong passwords and access controls	Automatically installing security patch updates on all components, including firmware, software, communications, and interfaces	Ensuring full backup of data and recovery mechanisms	Ensuring that there are no weak links between components
Firewalls			Implementing fail safe and manual overrides on all systems
Audit trails			

Source: Authors, derived from Martínez-Ballesté *et al*. (2013) and Cerrudo (2015).

While these security measures have genuine utility, they are far from a complete solution, particularly as smart technologies become ever more critical to smooth functioning of cities. Instead, a more systemic approach needs to be adopted in relation to both technical design and training. In particular, a s*ecurity-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 (Lomas, 2015); including a pilot phase within a living lab environment that includes testing the security of a product 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 on-going 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.

With respect to overseeing the security aspects of smart city technologies we would advocate the formation of a core security team within urban administrations with specialist skills and responsibilities above and beyond day-to-day IT-administration. The work of this team would include: undertaking wide-ranging threat and risk modelling; actively testing the security of smart city technologies (rather than simply monitoring and trusting vendor reassurances); conducting on-going security assessments; prepare and review 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 incident (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 should create 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 security teams or CERTs and are therefore underprepared to deal with a serious cyberattack.

In addition, a step-change in education and training vis-à-vis cybersecurity is required for all those involved in smart city ventures. Within local government and public service / infrastructure providers advanced security training should be developed and implemented across the organisation, but especially for those involved in the procurement, rollout and daily running of smart city technologies. This is important because although a system might have an extensive and robust set of technical security solutions these can be nullified by social exploits or human error. Similarly, such programmes should be instituted for developers and vendors to stress the need for a security-by-design approach, especially for start-ups and SMEs who might not have the in-house capacity for security expertise. In both cases, training needs to be part of a continual programme of professional development to refresh best practice and keep abreast of new technologies and vulnerabilities. We have found very little evidence of such system-wide security training programmes other than relatively light introductory courses, often taken on a one-off basis.

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 enacted and enforced. Therefore, there is a need to think about the most appropriate mechanisms to incentivise participation by both the public and commercial sector, and to penalise those who fail to improve security of their products, systems and services. In general, there are two routes to improving mitigation measures: market-led adoption and government-led regulation and legal enforcement.

The market-led approach consists of 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, and 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 would be driven by competition, fear of reputational damage and litigation caused by a major security scandal, and the benefits of self-regulation rather than a stick-approach of enforcement through legal

penalties and fines. While a market-led approach to security does presently exist, it predominately adopts the weak mitigation approach detailed above and not security-by-design. In part this is because there is currently 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 should be accompanied by more 'top-down' regulation and better management practices by city authorities and urban infrastructure 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, and loss of contract. There are now a host of smart city standards initiatives underway – by bodies such as the International Standards Organisation, British Standards Institute, American National Standards Institute, 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. For example, large public bodies operating the EU have to institute an audit and risk committee that identifies vulnerabilities and monitors potential threats to an organisation and oversees mitigation strategies. These are often broad in scope and could benefit from a sub-committee focused specifically on software security and network threats. This sub-committee should oversee and audit the work of the core security team; advise on the work priorities and programme; certify security assessments and that the city's smart city technologies conform to legal and regulatory requirements; ensure that response and mitigation plans and processes are in place; and ensure there is clear communication to public concerning how the security of smart city systems (Nanni, 2013). In addition, city administrations should bake security-by-design and on-going security maintenance (including on-time patching and 24/7 incident response) into the procurement process and subsequent service level contracts, with the extent to which the proposed solutions meet desired parameters directly influencing the evaluation of tenders (Cerrudo, 2015). They should also support whistle-blowers who wish to expose security vulnerabilities and require the public reporting of security breaches.

We have found no example of a city that presently enacts such systemic, enhanced security oversight or procurement beyond seeking existing mitigation strategies. For the most

part this is due to a lack of in-depth knowledge and competence, and institutional inertia. Consequently, smart city technologies have been in the past and are still being procured with little coordinated consideration of security harms and slotted into existing city management in an ad hoc fashion with minimal strategic foresight. Given the potential harms and the associated costs that can arise, this piecemeal and make-do approach needs to be discontinued to be replaced with a more systemic and coordinated approach.

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 materialising 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 labelled 'backward looking' and 'out-of-date', and derided for having a neo-Luddite mentality (see Jones, 2013). Indeed, at present, advocating a preventative approach would be considered a radical means of securing smart cities as it requires a reframing of the value around technology and a rethinking of the balance between 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 potential risks networked infrastructure pose, plus the cybersecurity, management and training costs of ensuring security, outweigh the efficiency and functionality gains promised and the 'inconveniences' of maintaining 'air-gapped' technologies (that is, systems that are physically isolated from other networks). Having to send a person physically to a component to re-activate it, reconfigure settings, or repair it, might seem costly and burdensome when it could be done remotely. Indeed, in the era of ubiquitous connectivity, cloud-computing, integrated and interoperable systems, remote control, the notion of having an air gap in critical 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 perils (Townsend, 2013; Greenfield, 2013; Kitchin, 2014; Datta, 2015). Certainly many existing smart city system deployment have not delivered the anticipated gains in efficiency, flexibility, productivity and convenience; in many cases, especially with regards to the Internet of Things, objects and systems have been digitally networked for little perceivable gain or real benefits to the functioning and management of cities (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 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 security risks.

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 recognised as the 'bleeding-edge' of insecurity.

Conclusion

In this paper we have examined in-depth the current state of play with regards to 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 in present day cities, yet they paradoxically create new risks, including making city infrastructure and services insecure, brittle, and open to extensive forms of vandalism, disruption and criminal exploitation. This paradox has largely been ignored by commercial and governmental interests or tackled through a traditional mitigation approach. This is perhaps no surprise. Although we have identified five forms of vulnerability and detailed the present extent of cyberattacks on city infrastructure and

services, presenting a number of illustrative examples where they have been compromised, as far as is publicly known the majority of attacks are presently being repulsed using cybersecurity software tools and management practices, or their effects have been only locally disruptive or damaging but not critical for the long term delivery of services (Singer & Friedman, 2014). Indeed, despite wide scale low-level attempts, successful cyberattacks on city systems are still relatively rare and when they have occurred their effects generally last no more than a few hours or involve the theft of data rather than creating life threatening situations. That said, even short term disturbances, such as the shutting down the electricity grid for a few hours or causing traffic gridlock, can be an expensive disruption through lost productivity and opportunities, and can also be potentially life-threatening. They also signal the threat of more damaging cyberattacks in coming years as actors develop more sophisticated methods of hacking and security measures fail to keep pace.

Indeed, it is clear that smart city technologies presently have multiple vulnerabilities and that these are and will be exploited for various ends. Moreover, there is a cybersecurity 'arms race' underway between attackers and defenders, and it maybe 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). In other words, smart city technologies are vulnerable to cyberattack and cyberterrorism and existing vulnerabilities are only likely to increase in the future. In our view, present strategies for addressing the vulnerabilities and risks posed by the mass adoption of networked technologies for city management are woefully inadequate and predominantly rely on existing technical and training mitigation strategies and market-led solutions.

Instead, we advocate 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 and responsibilities beyond general IT-administration, and a step-change in security training and continuing professional development in both public and commercial sectors. 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. We also suggest that serious consideration is 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 self-evidently too late to roll-back the smart city agenda and much of the adoption of smart city technologies by municipal authorities across the world cannot simply be removed. However, it is not too late to recognize the extent of the new security vulnerabilities, threats and risks posed by these technologies and to put in place strategies and approaches to mitigate and prevent them. We believe that not enough is presently being done by vendors and city administrations to identify vulnerabilities and risks and to formulate effective responses. Vandals, criminals and terrorists will undoubtedly continue to adapt their methods to exploit the layering of software dependent infrastructures throughout urban space, consequently much more attention needs to be focused on creating secure smart cities.

Acknowledgements

The research for this paper was funded by an ERC Advanced Investigator award (ERC-2012-AdG 323636-SOFTCITY) and by the Data Forum of the Department of the Taoiseach, Ireland, for a study entitled: 'Getting Smarter about Smart Cities: Improving Data Privacy and Data Security'.

References

Anand, Priya. (2016). The 'Mind-Boggling' Risks your City Faces from Cyber Attackers. *Market Watch*, 30 January. Retrieved from www.marketwatch.com/story/the-mind-boggling-risks-your-city-faces-from-cyber-attackers-2016-01-04

Article 29 DPWP. (2014). *Opinion 8/2014 on the Recent Developments on the Internet of Things*. Article 29 Data Protection Working Party. Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Beck, Ulrich. (1992). *Risk Society: Towards a New Modernity*. London: Sage.

Bellovin, Steven M. (2016). Attack Surfaces. *IEEE Security & Privacy*, 14(3), 88.

Bodenheim, Roland, Butts, Jonathan, Dunlap, Stephen, and Mullins, Barry. (2014). Evaluation of the Ability of the Shodan Search Engine to Identify Internet-facing Industrial Control Devices. *International Journal of Critical Infrastructure Protection*, 7, 114-123.

Cerrudo, Cesar. (2014) Hacking US (and UK, Australia, France, etc.) Traffic Control Systems. *IOActive Blog*, 30 April. http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html

Cerrudo, Cesar. (2015). An Emerging US (and world) Threat: Cities Wide Open to Cyber Attacks. *Securing Smart Cities*. Retrieved from http://securingsmartcities.org/wp-content/uploads/2015/05/CitiesWideOpenToCyberAttacks.pdf

Chacos, Brad. (2016). Osram's Lightify Smart Bulbs Suffer from Several Serious Security Flaws. *PC World*, 27 July. www.pcworld.com/article/3101008/connected-home/osrams-lightify-smart-bulbs-suffer-from-several-serious-security-flaws.html

Cox, Joseph. (2014). This Website Streams Camera Footage from Users Who Didn't Change Their Password. *Motherboard*, 31 October. Retrieved from http://motherboard.vice.com/read/this-website-streams-camera-footage-from-users-who-didnt-change-their-password

Datta, Ayona. (2015). New Urban Utopias of Postcolonial India: 'Entrepreneurial Urbanization' in Dholera Smart City, Gujarat. *Dialogues in Human Geography*, 5(1), 3-22.

Dodge, Martin, Kitchin, Rob. (2005). Codes of Life: Identification Codes and the Machine-Readable World. *Environment and Planning D: Society and Space*, 23(6), 851-881.

Durbin, Steve. (2015). Building smart city security. *TechCrunch*, 12 September. Retrieved from www.techcrunch.com/2015/09/12/building-smart-city-security

Evans, David J, and Herbert, David T. (1989). *Geography of Crime.* London: Routledge.

Frith, Jordan. (2105). Communicating Behind the Scenes: A Primer on Radio Frequency Identification (RFID). *Mobile Media & Communication*, 3(1), 91-105.

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*. Retrieved from www.usenix.org/system/files/conference/woot14/woot14-ghena.pdf

Gibbs, Samuel. 2016. Ransomware Attack on San Francisco Public transit Gives Everyone a Free Ride. *Guardian*, 28 November. Retrieved from www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware

Goodman, Marc. (2015). *Future Crimes.* New York: Bantam Press.

Greenburg, Andy. (2015) Hackers Remotely Kill a Jeep on the Highway—With Me in It. *Wired*, 21 July. Retrieved from www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

Greenfield, Adam. (2013). *Against the Smart City*. New York: Do Publications.

Greenwald, Glenn. (2014). *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State.* New York: Macmillan.

Hall, Tim, (2013). Geographies of the Illicit: Globalization and Organized Crime. *Progress in Human Geography*, 37(3), 366-685.

Hern, Alex. (2016). Ransomware Threat on the Rise. *Guardian*, 3 August. Retrieved from www.theguardian.com/technology/2016/aug/03/ransomware-threat-on-the-rise-as-40-of-businesses-attacked

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

Kitchin, Rob. (2014). The Real-Time City? Big Data and Smart Urbanism. *GeoJournal*, 79(1), 1-14.

Kitchin, Rob. (2016). The Ethics of Smart Cities and Urban Science. *Philosophical Transactions A*, 374(2083), 1-15.

Kitchin, Rob, Dodge, Martin. (2011). *Code/Space: Software and Everyday Life*. Cambridge, MA: MIT Press.

LeBeau, James L., Leitner, Michael. (2011). Progress in Research on the Geography of Crime. *The Professional Geographer*, 63(2), 161-173.

Levy, Steven. (1984). *Hackers: Heroes of the Computer Revolution*. Harmondsworth, UK: Penguin.

Li, Paul Luo, Shaw Mary, Herbsleb Jim, Ray Bonnie, Santhanam Peter. (2004). Empirical Evaluation of Defect Projection Models for Widely-deployed Production Software Systems. *ACM SIGSOFT Software Engineering Notes*, 29(6), 263-272.

Little, Richard G., (2010). Managing the Risk of Cascading Failure in Complex Urban Infrastructures. In Graham, Stephen, editor, *Disrupted Cities: When Infrastructure Fails.* London: Routledge, 27-39.

Lomas, Natasha (2015). The FTC Warns Internet Of Things Businesses To Bake In Privacy And Security. *TechCrunch*, 8 January. Retrieved from http://techcrunch.com/2015/01/08/ftc-iot-privacy-warning

MacKinnon, Danny, and Derickson, Kate D. (2013). From Resilience to Resourcefulness: A Critique of Resilience Policy and Activism. *Progress in Human Geography* 37(2), 253-270.

Manaugh, Geoff, (2016). *A Burglar's Guide to the City.* New York: Farrar, Straus and Giroux.

Markey, Edward J., Waxman, Henry A. (2013) *Electric Grid Vulnerability: Industry Response Reveal Security Gaps*. Retrieved from www.markey.senate.gov/imo/media/doc/Markey%20Grid%20Report_05.21.131.pdf

Martínez-Ballesté, Antoni., Pérez-Martínez, Pablo .A., Solanas, Agusti. (2013). The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City is Possible. *IEEE Communications Magazine*, 51(6), 136-141.

Nanni, Giampiero. (2013). *Transformational 'Smart Cities': Cyber Security and Resilience*. Mountain View, CA: Symantec.

Owens, William A., Dam, Kenneth W., and Lin, Herbert S. (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington DC: Committee on Offensive Information Warfare; National Research Council, National Academic Press.

Paganini, Pierluigi. (2013). Israeli Road Control System hacked, Caused Traffic Jam on Haifa Highway. *Hacker News*, 28 October. Retrieved from http://thehackernews.com/2013/10/israeli-road-control-system-hacked.html

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

Rainie, Lee., Anders, Janna., Connolly, Jennifer. (2014). Cyber Attacks Likely to Increase. *Digital Life in 2025.* Pew Research Center. Retrieved from www.pewinternet.org/files/2014/10/PI_FutureofCyberattacks_102914_pdf.pdf

Reilly, Steve. (2015). Records: Energy Department Struck by Cyber Attacks. *USA Today*, 11 September 2015. Retrieved from www.usatoday.com/story/news/2015/09/09/cyber-attacks-doe-energy/71929786/

Sarma, Sanjay. (2015). I Helped Invent the Internet of Things. Here's Why I'm Worried About How Secure it is. *Politico*, June 2015. Retrieved from www.politico.com/agenda/story/2015/06/internet-of-things-privacy-risks-security-000096

Schneier, Bruce. (2003). *Beyond Fear: Thinking sensibly about security in an uncertain world*. New York, Copernicus Books.

Singer, Peter W., Friedman, Allan. (2014). *Cybersecurity and Cyberwar.* Oxford: Oxford University Press.

Singh, Indu B., Pelton, Joseph N., (2013). Securing the Cyber City of the Future. *The Futurist*, 47(6), 22.

Söderström, Ola, Till Paasche, and Francisco Klauser, (2014). Smart Cities as Corporate Storytelling. *City* 18(3), 307-20.

Townsend, Anthony M., (2013). *Smart Cities: Big data, civic hackers and the quest for a new utopia*. New York, WW Norton and Company.

White, James M, (2016). Anticipatory Logics of the Smart City's Global Imaginary. *Urban Geography*, 37(4), 572-589.

Woolf, Nicky. (2016). DDoS Attack that disrupted Internet was Largest of its Kind in History. *Guardian,* 26 October. Retrieved from www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

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

Zetter, Kim. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *Wired News*, 3 March. Retrieved from www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid