3rd International Conference

on Public Policy (ICPP3)

June 28-30, 2017 – Singapore

Panel T09P04 Session 1

Smart Cities in Asia

Title of the paper

Mirror, mirror on the wall, who is the smartest of them all? Asian smart cities: urban challenges, digital vulnerabilities and policy re-adjustments

Author(s)

Teck Boon Tan, RSIS, NTU, Singapore, istbtan@ntu.edu.sg

Yu-Min Joo, LKYSPP, NUS, Singapore, sppjym@nus.edu.sg

Date of presentation

June 28th, 2017.

Mirror, mirror on the wall, who is the smartest of them all? Asian smart cities: urban challenges, digital vulnerabilities and policy re-adjustments

ABSTRACT:

Rooted in the seductive vision of a techno-utopian world, smart cities are today recognized as potentially the key to our urban malaise. Looking close though, we find that these high-tech urban architectures also harbor serious digital vulnerabilities rendering them susceptible to large-scale cyberattacks. Despite the severity of the problem, there is a dearth of systematic research to pinpoint these critical digital loopholes within the smart city architecture. The aim of this paper is to fill the gap by introducing a pool of empirical evidence to argue that smart cities are not adequately secure from large-scale cyberattacks and thus, unsafe for their citizens at the moment. It goes on to argue that smart city governments need to introduce a risk management approach to address this pressing policy issue.

KEYWORDS: smart cities; digital security; urban technology; cyber attacks

Introduction

Smart cities – broadly defined as urban spaces transformed by innovative digital technology – are springing up in almost every corners of the world (Glasmeier and Christopherson, 2015; Chen, 2010; Komninos et al., 2013). Reflecting the ongoing romance between policymakers and smart cities, there are now at least 33 such modern urban architectures globally with at least 55 more expected by 2025 (Cooley, 2014; Arrowsmith, 2014). In these high-tech urban architectures, digital technology is woven into every aspect of its operations including healthcare, public transportation, power supply, water management, e-government, telecommunications and so forth. The objective? To reconcile rapid urbanization with a multitude of public policy goals such as environmental sustainability, resource efficiency, improved urban livability, and even democratic governance (Stratigea et al., 2015; Albino, 2015; Luque-Ayala and Marvin, 2015; Townsend, 2013). As a seductive vision to help humanity cope with the myriad challenges rising alongside rapid urban growth, it is no wonder that smart cities are making their presence felt now and undoubtedly, will continue to do so in the coming years – albeit in varying forms.

However, the overwhelming collection of digital technologies underpinning the smart city can also lead to its downfall. No digital system in use today is 100 percent secure and there are indications that malicious hackers – motivated by monetary or political reasons – might be capable of exploiting systemic digital vulnerabilities in the smart city architecture to great effects (Cerrudo, 2015; Goodman, 2016). In their "fast and furious" pace to build smart cities, policymakers have unwittingly overlooked digital security, with cybersecurity turning into an afterthought rather than a primary focus from the outset. Consequently, smart cities have come to harbor critical digital vulnerabilities that expose them to large-scale cyberattacks. In the worst-

case scenario, malicious actors might be able to exploit systemic digital weaknesses in the smart city architecture to take down critical infrastructure systems. The outcome of such an attack is likely to be catastrophic with prolonged disruption of essential city services, significant economic losses and even civilian casualties (Clark et al., 2014). This unsettling picture is not imaginary because such an attack already happened in 2009, when hackers sabotaged the centrifuges in Iran's uranium enrichment facility in Natanz (Zetter, 2014). Further signaling the rise of this cyber-physical threat, a cyberattack then took down Ukraine's power grid in December 2015 leaving nearly 230,000 Ukrainians without power for hours (Zetter, 2016).

In spite of the growing threat, research into the digital security of smart cities remains in its infancy and because of that, there is a dearth of systematic inquiries. On the other hand, the prevailing techno-centric perspective in the smart city literature has persisted to portray smart cities as not only a positive development but also as a potentially transformational solution to rapid urbanization, environmental degradation, and resource depletion (Luque-Ayala and Marvin, 2015; Harrison et al., 2010). In view of their digital vulnerabilities, not only is this irresponsible, it is potentially deadly. To be fair, some scholars have taken issue with this fixation with 'technological fix' by drawing attention to its convenient disregard for the deep-rooted institutional and socio-human dynamics behind the development of smart cities (Nam and Pardo, 2011; Greenfield, 2013; Halpern et al, 2013). The inevitable outcome however, of this critical shift away from the techno-centric focus is that it has also resulted in the lack of systematic analysis on the technology embedded in smart cities, especially the digital security component.

What are the most critical digital vulnerabilities in the smart city architecture? How might city policymakers respond? By answering these questions in this paper, our research fills in an

important gap in the smart city literature and supports ongoing efforts to keep our smart cities safe. For sure, these issues are not limited to smart cities in Asia. Any smart city projects across the world should be aware of potential security flaws and digital insecurity. But a number of Asian smart cities in particular are being planned and delivered top-down, instead of being largely driven by small scale initiatives driven bottom-up. The upshot is that the large-scale smart city plans pushed forward in a "fast and furious" manner – oftentimes, with much global attention – could make cybersecurity issues more complex and pronounced. Furthermore, the general tendency of government's strong engagement involving projects in Asia further invites policy discussions on smart city cybersecurity. Among Asian smart cities, we specifically refer to the well-known cases of Songdo (in South Korea), a smart city built from scratch on green field, Hong Kong's smart city vision and Singapore's Smart Nation project, in order to situate our findings of key digital vulnerabilities of smart cities in a solid context. However, it is important to note that the three cities are used only for illustration purposes – to show the kinds of digital vulnerabilities that can be found in specific smart city technologies and the possible remedial policy actions needed to keep smart cities safe. We want to emphasize that they are *not* chosen for being special cases where cybersecurity is a particular issue. In fact, we emphasize again that this topic is important precisely because all smart cities are susceptible to large-scale cyberattacks and hence, need to be implemented with careful policy considerations.

Setting the scene: Refocusing on technology in the smart city discourse

The smart city concept has been promoted by the corporate sector and city governments as the new urban panacea to a multitude of urban woes like overcrowding, environmental degradation, resource depletion, rising crime rates and even poor healthcare outcome (Hollands, 2015: 62;

Townsend, 2014; Newman, 2016; Deakin and Waer, 2012; Tomitsch and Hauesler, 2015). Deeply rooted in the seductive vision of a techno-utopian world where digital technology is not only positive but potentially transformational, the smart city is an urban environment where information communication technology (ICT), big data, urban apps, intelligent infrastructure and industrial control systems are all brought together to facilitate real-time urban sensing, monitoring and management (Goodspeed, 2015; Luque-Ayala and Marvin, 2015). Belying this upbeat conception, there is however still much confusion in the scholarly literature over what exactly a smart city is (Caragliu et al., 2011; Cooley, 2014; Albino et al, 2015; Lee et al., 2014).

In all fairness, the task of formulating a working definition is greatly complicated by the fact that smart cities are often conceived under varying histories, contexts and agendas (Kitchin, 2015). Indeed, some smart cities were built from the ground up as showcase projects for green and ecological technology. Reflective of this theme, Songdo in South Korea and Masdar City in the United Arab Emirates are entirely new cities built on greenfield land (Shwayri, 2013; Goldenberg, 2016; Glasmeier and Christopherson, 2015). Then, there are those that were implanted into pre-existing urban centers to take advantage of the smart city concept as a sustainable model for urban development and renewal, among other things (Anthopoulos, 2017; Newcombe, 2014). Meanwhile, the policy agendas of smart cities also vary greatly from environmental sustainability (e.g., Vienna and San Diego) to inclusive governance (e.g., Seoul and Tallinn) to economic competitiveness (e.g., Hong Kong, Singapore, and Songdo). Despite the variations, smart cities do share some common features, and they can largely be grouped under the following three points of view.

The first one draws attention to the technological dimension by underlining the smart city's implementation of a diverse collection of digital technologies to monitor, understand and

manage the urban environment (Komninos, 2002 & 2008; Hall, 2000; Washburn et al., 2010; Klein and Kaefer, 2008; Townsend, 2015: 15). The pervasive application of technology is thought to be able to solve a host of urban woes including traffic gridlocks, air pollution, and crime, among others (Hollands, 2015; Luque-Ayala and Marvin, 2015). Besides homes, buildings, and physical infrastructure, this "smartness" is also weaved into a vast collection of everyday objects such as household appliances, personal devices and city sensors to promote automation, energy efficiency, democratic access, and civic management (Hancke et. Al, 2013; Harrison et al., 2010; GhaffarianHoseini et al., 2013). Framed in this way, the techno-centric perspective of the smart city epitomizes a techno-utopian world where digital technology infused into the urban fabric is not only a tool for urban growth and management, but also a driver for transformative change (Luque-Ayala and Marvin, 2015).

The second body of work however, cautioned against this techno-centric perspective by arguing first and foremost that smart city technology fails to solve some of the most fundamental problems plaguing urban centers today (Albino et al., 2015; Holland, 2008). For example, smart cities are ill-equipped to deal with the myriad of social structural challenges such as skyrocketing property prices, dilapidating neighborhoods, and uneven provision of public services (Glasmeier and Christopherson, 2015). Issues pertaining to inequality are in fact expected to worsen with the onset of smart city projects, which in some cases are driven by gentrification (Graham, 2002; Datta, 2015). In this context, literature anchored in this perspective began to underscore the socio-human dimension – specifically, the citizens and their importance in building a smart city (Alawadhi et al., 2012; Nam and Pardo, 2011), with technology as but a tool to improve the urban experience for the citizens (Komninos, 2011; Shapiro, 2006; Hollands, 2008: 315). Indeed, while the techno-centric perspective is likely to remain a cornerstone of the smart city discourse

as the key underlying and driving force, over-emphasizing its contributions also risks crowding out whatever little space is left for ordinary citizens to have a hand in shaping technology to meet their needs (Hollands, 2015; Vanolo, 2013: Albino et al., 2015).

In a similar fashion, the third body of work also warned against looking at the smart city phenomenon purely from a techno-centric perspective by pointing out the importance of public institutions in the making of smart cities (Albino et al., 2015; Giffinger et al., 2007). Technology, according to this view, is but "a first step". What is required in tandem are the right institutional elements in bringing ICT into the urban space (Nam and Pardo, 2011: 286; Albino et al., 2015). Although smart city technology has been associated with enhancing public administration and public service deliveries – by helping to make them more efficient, accessible, and responsive, for instance – the enabling technologies alone do not make a city smart if it is deprived of a supportive administrative environment (Nam and Pardo, 2015: 286). By setting down a course of action, public institutions lay out the direction for government officials, and just as important, hold them accountable for the implementation. Without these institutions, it is entirely conceivable that government officials – at the national, state or city level – could inject their personal biases into the implementation process and in the worst-case scenario, initiate actions that serve only their political interests. Viewed in this way, institutions – not technology – rest at the heart of smart city development.

The division between the techno-centric, socio-human and institutional perspectives is apparent in the smart city literature. One could argue that this split has sapped our focus on the potential problems that technology itself can give rise to within the smart city architecture. If the smart city discourse is continuously centered on how good the technology is, why it is not enough and what more should there be, then there is little room for a critical evaluation of how

unsafe the technology might be. In this context, a few cybersecurity researchers and security professionals have begun to raise questions pertaining to the digital security of smart cities (Goodman, 2015; Clark et al., 2014) but currently, this debate is mostly limited to a small cadre of researchers and professionals fragmented across disciplinary lines. Even for the few notable exceptions that delve into this particular dimension, they are predominantly single-case studies on specific applications and canonical examples such as mobile telephones or industrial control systems (see, e.g., Wang et al., 2017; Viitanen et al., 2015; Zegras et al., 2015; Knapp, 2011). The dearth of systematic research on the digital insecurity of smart cities across a mix of contexts and cases not only limits the amount of empirical evidence and theoretical insights to assess the digital security of smart cities, but also potentially blinds city governments to how deadly the problem can be.

Our paper aims to fill this gap by introducing a body of empirical evidence on the assorted digital vulnerabilities in the smart city architecture. To this end, we examined up-to-date technical information on smart city technologies from a variety of sources, including trade magazines, official government documents and websites, reputable international newspapers, and academic publications. We also participated in a number of smart city conferences, cybersecurity symposiums and ICT trade seminars, and interviewed a number of senior government officials.[1] Triangulating our data from these heterogeneous sources, we were able to identify a total of seven critical digital vulnerabilities in the smart city architecture, which we illustrate in this paper with the specific examples of smart Songdo, Hong Kong and Singapore. By drawing out these digital vulnerabilities and shedding light on their policy implications, this paper adds an important techno-security dimension to the ongoing smart city discourses.

[1] To ensure their privacy and willingness to talk, we have omitted their names herein and their views are presented as anonymous.

Digital vulnerabilities of smart cities

The three fundamental vulnerabilities of smart cities that we identified are: 1) hyper-connectivity, 2) attack surface, and 3) big data and Cloud-based data storage. These are also the essence of smart cities; smart cities are about 'everything' being 'connected' to each other, collecting and using 'big data' to transform daily urban living experience. However, it is important to emphasize that the increased connectivity, extended attack surface, and Cloud data security – core enabling components of the smart city – also pose new digital vulnerabilities. In addition, we were also able to isolate four more specific sub-categories of vulnerabilities pertaining to both the 'connectivity' and 'attack surface' of the smart city architecture. They are 1) exposed units, 2) resource-constraint devices, 3) mass-produced technology, and 4) long life-cycle and inadequate adoption of technology. In this section, we introduce each of these seven vulnerabilities, including their roles and connections to smart city architecture, why and how they expose the smart city architecture to cyberattacks.

First, central to the smart city concept, as well as its vulnerabilities, is the extensive application of wireless technology to bring about hyper-connectivity allowing constant communication of embedded systems and exchange of data. As a core feature of the smart city architecture, wireless technology (i.e., Bluetooth, Wi-Fi, WPAN, 802.15.4 and NFC) is a cost-efficient mode of communication that facilitates rapid network expansion allowing more devices to be added to a network without having to lay more crossover cables (Merritt, 2017). Wireless connectivity also allows for hyper-connectivity, which refers to the digital state of things where every smart sensor, device, and system in a network is connected to each other at all times

(CybeRisk, 2016). By enabling not just person-to-person (P2P) and person-to-machine (P2M) but machine-to-machine (M2M) communications, the policy decision to introduce and implement hyper-connectivity has enabled city managers to streamline and automate many essential public services in the smart city architecture.

While the wireless technology that facilitates hyper-connectivity is a crucial element in smart city architecture, it has at the same time also opened up the vast collection of digital sensors, devices and systems in the smart city architecture to so-called man-in-the-middle or MitM attacks (Zetter, 2015; Constantin, 2015). Unlike wired communication, which shares data over crossover cables for instance, it is possible to intercept wireless communication in the middle of the transmission of data. By positioning a signal interception instrument in the range of a smart sensor, devices or systems and then boosting its signal, criminals can trick a target sensor, device or system into 'believing' that the signal interception instrument is the legitimate receiver (Greenberg, 2015; Kolker, 2016). With this technique, a signal interception instrument is able to vacuum up the data transmitted by the target sensor, device or system. While it is illegal in many countries for private citizens to own or purchase signal interception instruments, these devices can be acquired through various unlawful and covert means (Gallagher, 2013).

Besides intercepting data during transfer, hackers armed with signal interception equipment are also capable of taking control of smart devices, remotely installing malware onto them without the owners' knowledge or even launching denial-of-service (DOS) attacks that prevent these devices from operating as per normal (Khandelwal, 2017; Tanner, 2014). Underscoring the susceptibility of wireless connectivity to hacking and manipulation, two security experts demonstrated in 2014 how they were able to take control of a vehicle by exploiting its Bluetooth vulnerability (DHS, 2015: 12). Even though one can argue that the

digital vulnerabilities inherent in wireless connectivity are not unique to the smart city architecture, the problem is greatly magnified in it due to among other things, the high-level of device heterogeneity.

Secondly, the unusually large attack surface of the smart city architecture is another major concern, our study finds. Defined as the sum of all the different points with which hackers can intrude into a network or digital environment, the attack surface of a smart city is immense for the reason that every sensor, device and system embedded in the smart city architecture is potentially a pathway for hackers to gain entry into the core networks of the smart city architecture. The ubiquitous technology that enables connectivity anytime and everywhere in our daily urban life is what defines a smart city. Everyday gadgets such as household appliances, personal computers (PCs) and smartphones, practically everything electrical – from pacemakers to thermostats to light bulbs to parking sensors – is becoming 'smart' and going online thanks to a tiny built-in microcontroller (which is a small special purpose computer) that makes control over the Internet possible. Although they are a mandatory feature of the smart city, this overwhelming collection of smart gadgets invariably creates more pathways for cyber manipulations (Clark et al., 2014: 7-10).

Giving a sense of the size of this attack surface, Evans (2011: 3) noted that in 2015, some 25 billion smart sensors, devices and systems were already in use around the world; by 2020, that figure is projected to hit a staggering 50 billion. And each one can, in theory, be a point of entry for hackers out to disrupt the smart city's critical infrastructure systems and core networks. Smart sensors are especially vulnerable in that they often lack the most basic cybersecurity features such as firewalls, antivirus, and authentication protocols (West, 2017). From these poorly secured sensors, it may be possible for hackers to find their way into more complex

systems such as the critical infrastructure and core networks of smart cities. Once in, the intruders might attempt to expropriate sensitive data stored in these systems. Alternatively, hackers could inject a ransomware to encrypt all the files stored in these systems rendering them irretrievable until a ransom is paid (Zetter, 2016). They might also attempt to take control of these systems crashing or disrupting them at will to wreck large-scale chaos and panic (Goodman, 2016). Whichever way, the outcome of such a breach will be dire, not to mention how it will likely undermine confidence in the safety of the smart city architecture.

Thirdly, the decision by smart city managers to move substantial amount of the data exhaust from the smart city architecture to the Cloud has also created a major digital vulnerability. From the sleeping habits of residents and their energy consumption patterns to city-wide traffic conditions and pollution levels, this data trove includes a rich mix of the most mundane, personal and sensitive (Bosch, 2014: 1352; Khatoun and Zeadally, 2016: 52). The benefits of cloud storage are certainly well reported (Center for Digital Government, 2016). From the perspective of city managers, the cloud offers on-demand and scalable storage capacity. In other words, as the volume of data surges, the service can be scaled up and drawn upon only when needed. Specifically, by eliminating the need for city managers to expand their own in-house storage infrastructure, cloud-based data storage offers a cost-efficient way of storing data as the volume of data surges. Additionally, by unpacking this so-called big data, city officials can provide better public services and manage their cities more efficiently. For example, they can spot the next traffic congestion and implement remedial actions – such as redirecting traffic – even before the gridlock takes shape (Epstein, 2015). Realizing the significance of this data trove for the management of smart cities, city managers have been turning to the cloud for a

cost-effective data storage solution as the volume of data exhaust grows exponentially (Reinsel et al., 2017: 3). That in turn has created a gaping digital loophole in the smart city architecture.

The mass migration of city-level data to the Cloud also has a downside in that the onus of digital security falls squarely on the cloud service providers (CSPs). If these providers of the cloud servers fail to put in place rigorous data security standards, then they risk exposing their storage hardware to cyber-attacks and data theft (Palo Alto Networks, 2016). Even more unsettling is that evidence suggests hackers are increasingly turning their focus onto cloud-based storage solutions (Denisco, 2017; Newman, 2017). In view of the great variety and vast amount of information stored in these servers, a breach will not only result in massive data loss but also compromise sensitive information. Certainly, high profile breaches involving several celebrities in 2014 underlined the pitfalls of Cloud-based storage (McCormick, 2014). Often located in different parts of the world, these cloud servers are also extremely hard to secure. With no jurisdiction or direct ownership, city managers will have to rely exclusively on the CSPs to secure their data storage hardware from cyber intrusions – an undertaking which they have visibly failed from time to time (Conger, 2016; Gibbs, 2016).

In addition, our analysis indicates that four groups of possible specific vulnerabilities that are related to the core vulnerabilities of ‘connectivity’ and ‘attack surface’. Overlooked by city managers and smart city technology suppliers is the sheer number of physically exposed units (Henn, 2016). As a citywide integrated system, smart cities are retrofitted with numerous digital sensors, devices, and systems placed sometimes in remote areas under wide-open conditions as they are weaved into the smart city architecture. Especially when it concerns environmental issues of energy efficiency (e.g., smart streetlights, energy meters, parking sensors), pollution detectors, etc., or when a smart city is more spread-out (as opposed to being densely populated),

smart city technologies could end up being deployed in remote and open areas, exposed to tampering by malicious actors.

Secondly, many sensors and devices embedded in the smart city architecture are resource constrained and hence, susceptible to digital intrusions since they lack proper protection against increasingly sophisticated malwares. Smart city's ubiquitous computing has resulted in an increased number of common and daily use electronic gadgets as well as small sensors integrated into the smart city system. Although on the whole, this embedded technology represents a much more sophisticated and high-tech system, it also means that resource-constraint units of small everyday objects and sensors are invariably introduced into the system. Though labelled as 'smart', these resource-constrained sensors and devices are in reality surprisingly quite unsophisticated, with only limited processing, storage, encryption and authentication capabilities.

At present, to avoid unauthorized access and data interception, networks that rely on wireless communications utilize encryption and pre-shared authentication – a process in which default passwords are used to identify discrete devices and share data (Shinder, 2001). The problem is that resource-constrained devices and sensors lack antivirus and firewall protection (West, 2017). By virtue of their low computing power, compact sizes and low manufacturing cost, it is practically impossible to incorporate strong security features into these units (Bicchierai, 2016). Without strong security features, these units are dangerously vulnerable to increasingly sophisticated malware such as *Mirai*, a software virus of sort that travels on its own across cyberspace targeting poorly secured Internet-enabled gadgets (Newman, 2016). Patching resource-constrained units after they had rolled off the assembly line is also not an option given their parsimonious designs (Shakarian et al., 2013: 202). Their sheer numbers further compound the security challenge posed. With millions of them already integrated into the smart city

architecture, patching all of them with the latest security updates will be a logistical nightmare, if not an impossible task.

Thirdly, the widespread use of mass-produced units also poses problems for the smart city architecture writ large (CybeRisk, 2016; Henn, 2013). Smart city technologies, acquired in large numbers, are likely to be mass-produced by a handful of leading technology multinationals with vested interest in various smart city initiatives. Internet-enabled household appliances, high-tech teleconference gadgets, smart parking sensors, smart streetlights, and RFID tags embedded in automobiles, are just a few of the many examples. Yet, mass production means that an entire product line will share the same digital vulnerabilities (DHS, 2015: 12). Once hackers figure out how to breach one unit, they will be able to replicate their method of attack across all other identical units, not just in one city, but also around the world.

If the designs of smart sensors, devices and systems allow them to be repaired the moment a digital flaw is uncovered, then the problem can be quickly contained and rectified. However, if these mass-produced units cannot be patched or repaired when vulnerabilities are uncovered – as in the case of resource-constrained units – then they can create a pathway for malicious hackers to penetrate other systems in the network (Siddiqui, 2015). The only solution in this case would be to replace the vulnerable units *en masse* – a solution that is likely to be costly, *if* it is feasible at all.

Fourthly, we find that a major digital flaw in the smart city architecture can arise from the long lifecycle of smart city technology (Cole, 2016) as well as its inconsistent adoption and replacement. Many of the sensors, devices, and systems in the smart city architecture have longer product lifecycles than consumer products. Laptop for example, at around 5.5 years and smartphones at around 4.6 years. The smart streetlight, for example, is expected to have a

lifespan of more than 11 years (GE, 2017). There is little incentive to make products with shorter lifecycle, when they are going to be owned and managed by city governments, more as a public good than a consumer good. City managers are not going to be interested in having the trendiest or newest technology by replacing the old ones quickly. Running on public tax money, cities are also more likely to exhibit (hopefully) more conservative spending patterns. The downside of this conservatism is that city governments often lack the motivation and resources to replace older technology with the latest one. Whatever the reason may be, a number of smart city technologies have extended lifecycles, and city governments have usually shown slower adoption and replacement of these technologies with newer and more secure ones.

It is not difficult to see that in an era in which technology becomes outdated within a short period, problems emerge when an older and less secure piece of smart city technologies are not replaced quickly enough by a newer and more secure versions. The outcome of this uneven migration to a superior piece of technology is that it can create momentary gaps in the digital ecosystem that malicious hackers can exploit to gain unauthorized entry into the smart city architecture (DHS, 2015: 14). In practical terms, manufacturers must roll out security updates regularly for as long as these technologies are in use – which may not always be the case. If their manufacturers fail to do so in a timely fashion, then hackers will be able to exploit that window of opportunity to breach units that have momentarily become digitally vulnerable (Chang, 2017).

All these vulnerabilities are connected and many potential problems that could arise in smart city projects relate to a combination of these key vulnerabilities. To illustrate them with concrete case study of smart cities, we now briefly introduce the cases of Songdo, Hong Kong and Singapore, and explore in what ways their smart technologies could potentially harbor some of the vulnerabilities listed in this section.

Songdo, Hong Kong and Singapore – anatomy of mega smart city projects

We choose to examine the Asian smart cities of Songdo, Hong Kong and Singapore because they represent the epitome of government-led smart city projects. At the same time, the three notable smart cities also offer a nice contrast since one was built from scratch – as in the case of Songdo – while Hong Kong and Singapore were implemented within a fully developed metropolis. In contrast, Singapore represents a modern infrastructure ecosystem whereas anecdotal evidence suggests that Hong Kong's infrastructure (especially housing) has been neglected for sometime. Underlining potential digital vulnerabilities of these cities would indicate that these threats are very real for both new and existing cities looking to implement the smart city vision.

Songdo

Together with PlanIT Valley (Portugal) and Masdar (United Emirates), Songdo in South Korea is a well-known smart city project built from scratch. More accurately, it is a pilot project of a 'ubiquitous city' in South Korea, and is built on 600 hectares of reclaimed land on the edge of the city of Incheon. Initially, it started off as a Free Economic Zone, seeking to attract international companies, but quickly embraced the smart city vision in 2004. POSCO and Gale International are the main developers of the city – both of whom wanted to develop Songdo as a global showroom and a testbed of smart city technology.

For the purpose of this paper, we selected some of the key smart city technologies implemented to establish what kind of potential digital vulnerabilities lie hidden. A major player, CISCO has been promoting its TelePresence solutions in a number of apartments, offices, and

even hotels in Songdo. The idea is that it would allow residents, visitors, and workers to use the customized television screens for remote video-conferencing with each other and take classes from instructors around the globe. The system involves multiple television screens connected to one another and as CISCO plans to expand its services, we can envision how mass-produced systems lacking in cybersecurity protection could potentially become an entry point for malicious hackers – motivated either by political or monetary reasons.

Secondly, Songdo has numerous sensors embedded in the city to monitor traffic conditions, as well as CCTV cameras to monitor traffic and crime. Set up in plain sight, each of the exposed and mass-produced sensors and CCTVs planted across the city are potential entry points for malicious actors. Looking closely, these units are not equipped with the kind of security mechanisms designed to stop malware and as a result of which, the images and data they send are not secured. One could also question whether and how often the government would be interested in updating and replacing the numerous sensors and CCTVs spread across the city. It is already very costly to place sensors and CCTVs for monitoring purposes in the first place. In this context, the government would not find it feasible to frequently replace and update sensors and CCTVs, thus rendering them more vulnerable to cyberattacks.

A prime case study is Songdo's pneumatic waste disposal system underground, which sucks trash via pipes into the underground facility where the trash is automatically sorted and then recycled or burned. Again, this high-tech system would not be easy to replace as it is costly to build, highly complex and massive in size. Because the city government would rather maintain it rather than replace it, it will have a long lifecycle. Without any garbage collection trucks, only seven employees are required to run the whole system for the city. One can only imagine what chaos it would bring if this critical system were hacked and shut down.

In fact, as critical infrastructure systems do not exist in complete isolation, a failure in one system can potentially create a cascading effect with catastrophic fallouts. Apart from the pneumatic waste disposal system, water-processing facilities, the power grid and even transportation systems can all be subverted in a cyberattack. Owing to policies that brought about hyper-connectivity, a handful of hackers can potentially bring down the entire smart city architecture simply by targeting everyday objects like sensors, CCTVs, and TelePresence units, etc., to find their way into more complex systems and networks.

Hong Kong

With its ageing infrastructure, overcrowding and skyrocketing property prices, Hong Kong has set the goal of becoming a smart city to improve the urban experience for its citizens. In this futuristic vision, the Special Administrative Region (SAR) of the People's Republic of China in East Asia is slated to deploy an array of digital technology, software apps and big data to cope with the challenges brought on my rapid urbanization and to some extent, years of neglect by previous administrations. Accordingly, the Hong Kong government wants a cleaner, sustainable and more livable city for its seven million plus citizens.

Signs of this transformation can already be seen throughout the autonomous region on the Pearl River Delta of China. First and foremost, the Hong Kong government wants to tackle air pollution, especially in the downtown areas for the reason that poor air quality has led to an increase in the number of days of hospital stays for respiratory illnesses and premature deaths. Apart from a smart parking system, it wants to enhance its road infrastructure for users through the implementation of an electronic road pricing system – as opposed to building more roads. It

is also looking to optimize its bus system to addressing the 'last-mile' problem and make the city's subway more attractive for car owners. Besides encouraging Hong Kong citizens who want to buy a car to go for hybrid or electric ones, it is encouraging them to walk and cycle to help the city cut down on carbon emissions.

On the digital front, Hong Kong has made great strides in terms of retrofitting the city with Internet access for its citizens. Our field study finds that some public buses have Internet access giving passengers the ability to check their emails, search for information and even download music and video while on the go. Subway stations in Hong Kong have Wi-Fi access points and passengers with smartphones and laptops can go online just by standing next to these machines. Overall, free Wi-Fi can easily be found in Hong Kong, especially in the downtown areas, in shopping malls and subway stations. Staying connected in Hong Kong is never an issue at all for anyone with a smartphone and that in itself, speaks to the high level of connectivity in the SAR.

As with any technological development in human history, the smart city technologies the Hong Kong government have introduced (or are planning to) their downside even as they deliver enormous benefits. In particular, extensive wireless connectivity entails no small risk for Hong Kong's smart city vision since it increases the danger of MitM attacks. Again, it is important to bear in mind that data theft is not the only concern in the smart city architecture but rather how resource-constrained units might be subverted by malicious hackers to carry out DoS attacks on other systems connected to the network. And since no system exists in isolation, a shut down in one can easily cascade to others with catastrophic consequences. In that sense, the extensive level of wireless connectivity (and easy access) in Hong Kong is a matter of serious concern from the standpoint of cybersecurity.

Singapore

Singapore's Smart Nation initiative was launched in 2014. The city-state in effect is already a bona fide smart city, with its smart streetlights, smart parking system, smart road fee collections, to just a name a few of its already existing smart services and infrastructure. What this latest and new initiative embodies is more holistic coordination and much more intensified effort to develop a hyper-connected and data-driven urban landscape. The fact that it is named a *Smart Nation* – as opposed to a smart city – captures what the essence of what the Singapore government is aiming for.

There are four major areas that have been implemented so far: e-payments, healthcare, transportation, and government services. These are all very critical systems with key information and data that needs to be securely protected. Especially when the smart nation involves building an integrated networks and platforms, such as national platform for telemedicine, National Digital Identity System for both public and private-sector service uses, and Central Addressing Scheme (allowing one to transfer money using mobile phone numbers) for e-payments, the issue of protecting the system from cyberattacks cannot be underestimated. In fact, SingPass (i.e., the national authentication system) that began in 2003 has encountered security issues, which included a breach of over 1000 user accounts in 2014, and the 'harvesting' of login credentials of SingPass users in 2011. These are just some of the examples of what could happen anywhere in the world with digitized systems.

Accordingly, the Singapore government is very much aware of the importance of cybersecurity issue. In 2015, it rolled out additional layer of security for SingPass, which now

requires a two-step identification (2FA) for important online transactions. Furthermore, as it rolls out the National Digital Identity System, GovTech (Government Technology Agency of Singapore) is actively seeking to update the nation's security system, including biometric encryption. More than anything else, these massive and critical integrated platforms require state-of-the-art security and protection - something that the Singapore government is very much aware of.

Singapore is also looking to build an integrated network of sensor across the city-state to collect various transportation and environmental data. Looking closely, it is conceivable that some of these sensors are susceptible to the digital threats discussed thus far – large numbers spread across the island, exposed locations, easy access for hackers, and the vulnerabilities stemming from their mass-produced nature and long-life cycles. Already, different agencies of Singapore government have a number of their sensors and cameras mounted on roadsides, train stations, street lamps, public housing estates, and in drainages, for their own use. What the Smart Nation will do is to build its Smart National Platform (SNP) as an integrated data source. While this will help Singapore to become one step closer to being a Smart Nation, connecting and consolidating all the sensors and data to tap into the central data source of SNP could increase its exposure to cyberattacks. It is important to bear in mind that if malicious hackers breached one of these sensors or cameras spread out across the island, the hacked device could potentially affect the functioning of other more complex systems for the reason that they are all interconnected.

What we can see from these three cases is that digital vulnerabilities are not theoretical and there is a pressing need for city managers to address them. Even though these canonical examples of Asian smart cities are implemented by capable and efficient governments, these

high-tech urban architectures are not free from digital vulnerabilities and cyberattacks. Hence, one is prompted to question how 'safe and secure' the relentless drive for smart city projects in Asia is. Any national or local government promoting smart cities should pause for a moment and carefully think through whether their smart cities are secure enough, and what they can do to tackle this digital insecurity. Based on our interviews and secondary research, we propose the most feasible remedial action in the next section.

Policy re-adjustments for the smart cities of tomorrow

We have seen so far that what defines smart cities – hyper-connectivity, increased surface attack, and Cloud – are the key sources of digital vulnerabilities. The question then is not how the problem can be solved, but how it can be managed since a plan to protect every one of the millions of digital sensors, devices and systems in the smart city architecture from cyberattacks is neither realistic nor practical. In the end, some cyberattacks are going to be successful and breaches are therefore inevitable. Supposedly, with sufficient financial support, a team of highly motivated hackers will be able to breach any digital system on this planet; in other words, no digital system in use today is 100 percent secure.

Therefore, we propose a risk management approach as the more pragmatic and coherent answer for city managers looking to safeguard their smart cities from large-scale digital intrusions. In practical terms, this means weighing the projected impact of a breach against the resources needed to stop it. The more critical a system is, the more resources it ought to receive. This approach reduces the monumental task of securing the smart city architecture from cyberattacks to something that is more manageable and viable, by streamlining what needs to be

protected the most. It forces city managers to examine critically the multitude of digital sensors, devices and systems in their smart city architecture, and zero in on those assessed to be the most vital. Without this informed process of risk management approach to cybersecurity, the chances of misallocating valuable resources for the protection of less essential systems can be rather high. By neatly delineating what the most critical systems are, it becomes possible to direct limited public resources efficiently for their protection.

To be sure, this risk management approach to the cyber defense of smart cities will certainly leave some systems vulnerable to digital intrusions. It can thus be complemented by the following policy adjustments. In particular, since hackers typically take the path of least resistance, a coherent cyber-defense policy in the smart city architecture should aim to raise the cost or consequences of their actions. Following this logic, city managers can, in theory, deter cyberattacks on their smart city architecture simply by making cyberattacks more painful, difficult and expensive for the hackers. Smart city managers also need to follow best practices for cybersecurity to make it significantly more challenging for hackers to gain entry into their core networks and critical infrastructures. It involves for example, making sure that legacy technologies are replaced in a timely manner. While city governments may never react fast enough to changing technology, they can at least minimize the risk of cyberattack on their smart city architecture by keeping pace with newer technology as opposed to leaving legacy technology indefinitely in place with no action taken to replace them. Other best practices include protecting smart city technologies with the most recent security patches, putting in place a recovery plan in the event of a breach and ensuring that employees as well as contractors follow strict cybersecurity guidelines – such as not connecting their personal USB flash drive

into their organizations' networks, not opening suspicious emails, not bringing poorly secured devices to work and so forth.

Meanwhile, smart city managers might be able to deter cyberattacks by increasing the risk of penalties for hackers. By making cyberattacks more painful and costly, it is possible for smart city managers to render their high-tech urban architectures less attractive to malicious hackers than those who do little to hold them accountable. Even so, the problem of attribution – defined as the process of establishing the identity and location of an attacker – often hamper efforts to bring those responsible for cyberattacks to justice. Cyberattacks are often – though not always – transboundary in nature meaning that hackers are frequently located far away from their targets. That not only made law enforcement investigations into cyberattacks nearly impossible but also compounded the challenge of indicting the perpetrators.

Nevertheless, by working in concert with international law enforcement and national governments, smart city managers would improve their chances of bringing malicious hackers to justice. Smart cities around the world should quite simply, work together as a collective to fend off hackers. Granted that some smart city technologies are mass-produced, it makes sense for smart city managers to band together since a successful attack on these technologies might also be replicated in smart cities across the world. By hardening their cyber-defense through joint investigation and prosecution, smart city managers – as a global collective – force malicious hackers to expend more of their time and resources to adapt thus raising the cost of their attacks. Sharing knowledge about new cyber threats and more importantly, cybersecurity solutions will also strengthen the ability of smart city managers to cope with an ever-evolving threat. At the end of the day, smart cities need not be impenetrable; they just have to be more secure than other

urban centers to tamper their appeal to hackers who after weighing the pros and cons, may well move on to other targets that are less hardened.

Conclusions

This paper highlighted how smart cities in Asia and around the world harbor digital vulnerabilities that expose them to large-scale cyberattacks. For one, the multitude of digital sensors, devices and systems has created an unusually large attack surface with each one of them presenting a possible point of entry for malicious hackers to work their way into the core networks of the smart city architecture. As more and more devices become networked and instrumented, physical infrastructure become more complex and automated, digital insecurity will become part of the urban landscape, and cyberattacks will invariably have an impact on the physical world. This apocalyptic scenario is not imaginary but very real.

Indeed, using the cases of Songdo, Hong Kong and Singapore, we have shown where and how the digital vulnerabilities might lie. But these cities are not the only ones exposed to cyberattacks, all smart city projects are vulnerable to digital manipulation and subversion. Seeing the complex assortment of deadly digital loopholes in the smart city architecture, we then suggested how smart city managers can respond to the digital vulnerabilities surfaced in this paper. The fact that Songdo, Hong Kong and Singapore are highly centralized in their development and management suggests that there are both threats and opportunities when it comes digital security. The massively connected smart systems and infrastructures pushed with much fanfare could invite cyberattacks, yet at the same time, the government could also have more leverage in protecting their cities once they have set their minds to do so, as they are deeply involved in the planning and construction of their smart cities. We do not provide an answer

herein as to which types of governance (i.e., centralized or decentralized) are more secure, let alone which specific cities are, in this paper. What we hope to do is to show why and how it is critical to pause and think about the digital vulnerabilities of smart cities, thus providing the necessary impetus and policy guidance for many Asian governments that are racing to jump onto the smart cities bandwagon.

Therefore, our answer to the question of 'who's the smartest of them all' is the one who makes a smarter move by putting in place a set of defensive strategies that are a step ahead of both intruders and other cities to fend off cyberattacks. As governments around the world scramble to build more smart cities, we argue that the 'smarter' or 'smartest' cities would be the ones that are digitally secure while addressing their urban challenges through smart city projects, rather than adopting the most advanced and new technology. In other words, smart-er(est) cities should not be measured by the scale and the degree of technology adoption, but how smart the technology solves the myriad of urban challenges facing a city in a safe and secure manner. Ultimately, cities that are vulnerable to cyberattacks will not be able to deliver the boundless urban futures that smart cities have promised us.

Bibliography

S. Alawadhi, A. Aldama-Nalda, H. Chourabi, J.R. Gil-Garcia, S. Leung, S. Mellouli, T. Nam, T.A. Pardo, H.J. Scholl, S. Walker, "Building Understanding of Smart City Initiatives," Lecture Notes in Computer Science 7443 (2012) 40–53.

V. Albino, U. Berardi and R.M. Dangelico, "Smart Cities, Definitions, Performance and

L. Anthopoulos, "Smart utopia vs. smart reality: Learning by experience from 10 smart city cases," *Cities* 63 (2017) 128-148.

L. Arrowsmith, "Smart Cities: Business Model, Technologies and Existing Projects." *IHS Technology* (2014).

L.F. Bicchierai, "Wannabe Hackers are Adding 'Terrible' and 'Stupid' Features to Mirai," *Motherboard* (October 27, 2016) <https://motherboard.vice.com/read/wannabe-hackers-are-adding-terrible-and-stupid-features-to-mirai> Accessed on Nov 8, 2016.

C. Bosch, "Securing the smart grid: Protecting national security and privacy through mandatory, enforceable interoperability standards," *Fordham Urban Law Journal*, 41:4 (2014) 1349-1406.

F. Caldeira, T. Cruz, P. Simoes and E. Monteiro, "Towards Protecting Critical Infrastructures," in *Cybersecurity Policies and Strategies for Cyberwarfare Prevention,* ed. Jean-Loup Richet, USA: IGI Global, 2015.

A. Caragliu, C.D. Bo, P. Nijkamp, "Smart Cities in Europe," *Journal of Urban Technology*, 18:2 (April 2011) 65-82.

Center for Digital Government, "Why more data is heading to the cloud," (2016) <https://afd34ee8b0806295b5a7-9fbee7de8d51db511b5de86d75069107.ssl.cf1.rackcdn.com/CDG16_BRIEF_SHI-V.PDF> Accessed on February 1, 2017.

C. Cerrudo, "Hacking Smart Cities," (paper presented at RSA Conference 2015, San Francisco, California, April 20 to 24). <https://www.rsaconference.com/writable/presentations/file_upload/hta-t10-hacking-smart-cities_final.pdf> Accessed on April 18, 2017.

V. Chang, "Wi-Fi security: When the router is the weakest link," *The Straits Times* (January 18, 2017) <http://www.straitstimes.com/tech/pcs/wi-fi-security-when-the-router-is-the-weak-link> Accessed on January 29, 2017.

T.M. Chen, "Smart Grids, Smart Cities Need Better Networks [Editor's Note]," *IEEE Network* 24: 2 (2010) 2–3.

D. Clark, T. Berson and H.S. Lin, eds., *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* (Washington D.C.: The National Academies Press, 2014).

B. Cole, "The Cyber Risk of Connected Vehicle Technology," *TechTarget* (February 2016) < http://internetofthingsagenda.techtarget.com/feature/The-cyber-risks-of-connected-vehicle-technology> Accessed on April 17, 2017.

K. Conger, "Microsoft triumphs in warrant case against US government," *TechCrunch* (July 14, 2016) <https://techcrunch.com/2016/07/14/microsoft-wins-second-circuit-warrant/> Accessed on November 17, 2016.

L. Constantin, "Researchers: IoT devices are not designed with security in mind," *InfoWorld* (April 7, 2016) <http://www.infoworld.com/article/2906641/security/researchers-iot-devices-are-not-designed-with-security-in-mind.html> Accessed on February 23, 2017.

D. Cooley, "Next Decade to Bring Fourfold Increase in the Number of Smart Cities," Smart Cities Council (August 6, 2014) < http://smartcitiescouncil.com/article/next-decade-bring-fourfold-increase-number-smart-cities> Accessed on April 29, 2017.

CybeRisk, "What Cyber Threats are Smart Cities Facing," *CybeRisk Security Solution* (November 7, 2016) <http://www.cyberisk.biz/what-cyber-threats-are-smart-cities-facing/> Accessed on January 31, 2017.

A. Datta, "New urban utopias of postcolonial India: 'Entrepreneurial urbanization' in Dholera smart city, Gujarat," *Dialogues in Human Geography*, 5:1 (2015) 3-22.

M. Deakin and H.A. Waer (eds), *From Intelligent to Smart Cities* (UK: Routledge, 2012).

A. Denisco, "Spam and cloud attacks rising, four steps to protect your business," *TechRepublic*, (January 31, 2017) <http://www.techrepublic.com/article/report-spam-and-cloud-attacks-rising-4-steps-to-protect-your business/?ftag=TRE684d531&bhid=27278421562336614541730716262481> Accessed on February 2, 2017.

E. Epstein, "2030: How four smart cities are gearing up for the future," *MashableAsia* (March 5, 2015) <http://mashable.com/2015/03/05/future-cities/#6iCWzdIH7sqb> Accessed on March 23, 2017.

D. Evans, "The Internet of Things: How the Evolution of the Internet is Changing Everything," *Cisco IBSG* (April 2011) <http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf> Accessed on January 9, 2017.

R. Gallagher, "Meet the machines that steal your phone's data," *Ars Technica* (September 26, 2013) <https://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/> Accessed on January 30, 2017.

GE, "Bright Lights, Brilliant Cities," *GE Digital* (2017) <http://www.ge.com/digital/blog/bright-lights-brilliant-cities> Accessed on November 10, 2016.

A. GhaffarianHoseini, U. Berardi, N. Dahlan, A. GhaffarianHoseini and N. Makaremi, "The Essence of Future Smart Houses: From Embedding ICT to Adapting to Sustainability Principles," *Renewable & Sustainable Energy Reviews* 24 (2013) 593-607.

S. Gibbs, "Dropbox hack leads to leaking of 68m user passwords on the Internet," *The Guardian* (August 31, 2016) < https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach> Accessed on April 2, 2017.

R. Giffinger, C. Fertner, H. Kramar, R. Kalasek, N. Pichler-Milanovic, and E. Meijers, Smart Cities: Ranking of European Medium-sized Cities (Vienna: Centre of Regional Science, 2007).

A. Glasmeier and S. Christopherson, "Thinking about Smart Cities," *Cambridge Journal of Regions, Economy and Society*, 8 (2015) 3-12.

S. Goldenberg, "Masdar's zero-carbon dream could become the world's first green ghost town," *The Guardian* (February 16, 2016) <https://www.theguardian.com/environment/2016/feb/16/masdars-zero-carbon-dream-could-become-worlds-first-green-ghost-town> Accessed on May 2, 2017.

M. Goodman, *Future Crimes: Inside the Digital Underground and the Battle for our Connected World* (New York: Anchor Books) 2016.

R. Goodspeed, "Smart cities: moving beyond urban cybernetics to tackle wicked problems," *Cambridge Journal of Regions, Economy and Society*, 8 (2015), 79–92.

S. Graham, "Bridging urban digital divides? Urban polarisation and information and communications technologies (ICTs)," *Urban Studies* 39:1 (2002) 33–56.

Greater London Authority, "Smart London Plan," *Mayor of London* (2013), <http://www.london.gov.uk/sites/default/files/smart_london_plan.pdf> Accessed on April 12, 2017.

A. Greenberg, "This Hacker's Tiny Device Unlocks Cars and Opens Garages," *WIRED* (August 6, 2015) <https://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/> Accessed on January 13, 2017.

A. Greenfield, *Against the Smart City* (New York: Do Projects, 2013).

R.E. Hall, "The vision of a smart city". In Proceedings of the 2nd International Life Extension Technology Workshop, Paris, France (September 28, 2000) <https://www.osti.gov/scitech/servlets/purl/773961> Accessed on May 4, 2017.

O. Halpern, J. LeCavalier and N. Calvillo, "Test-bed urbanism," *Public Culture* 25:2 (2013) 272–306.

G.P. Hancke, B.C. Silva, and G.P. Hancke, "The Role of Advanced Sensing in Smart Cities," *Sensors* 13 (2013) 393–425.

C. Harrison, B. Eckman, R. Hamilton, P. Hartswick, J. Kalagnanam, J. Paraszczak, and P. Williams, "Foundations for Smarter Cities," *IBM Journal of Research and Development* 54: 4 (2010) 1–16.

S. Henn, "Street lights, security systems and sewers? They are hackable too," *NPR* (March 4, 2013) <http://www.npr.org/sections/alltechconsidered/2013/03/04/173423493/street-lights-security-systems-and-sewers-theyre-hackable-too> Accessed on January 30, 2017.

R.G. Hollands, "Will the Real Smart City Stand Up?" *City*, 12:3 (2008) 302-320.

R.G. Hollands, "Critical interventions into the corporate smart city," *Cambridge Journal of Regions, Economy and Society*, 8 (2015) 61-77.

R. Khatoun and S. Zeadally, "Smart Cities: Concepts, Architecture and Research Opportunities," *Communications of the ACM* 59:8 (August 2016) 46-57.

R. Kitchin, "Making sense of smart cities: addressing present shortcomings," *Cambridge Journal of Regions, Economy and Society*, 8 (2015) 131-136.

C. Klein, and G. Kaefer, "From Smart Homes to Smart Cities: Opportunities and Challenges from an Industrial Perspective," Proc. of the 8th International Conference, NEW2AN and 1st Russian Conference on Smart Spaces, SMART 2008, St. Petersburg, Russia, September 3–5, 2008.

E. Knapp, *Industrial network security: securing critical infrastructure networks for Smart Grid, SCADA , and other industrial control systems,* (Waltham, MA: Syngress) 2011.

R. Kolker, "What happens when the surveillance state becomes an affordable gadget?" *Bloomberg* (March 10, 2016) <https://www.bloomberg.com/news/articles/2016-03-10/what-happens-when-the-surveillance-state-becomes-an-affordable-gadget> Accessed on March 30, 2017.

N. Komninos, *Intelligent Cities: Innovation, Knowledge Systems and Digital Spaces* (London: Routledge) 2002.

N. Komninos, "Intelligent Cities: Variable Geometries of Spatial Intelligence," *Intelligent Buildings International* 3: 3 (2011) 172–188.

N. Komninos, M. Pallot, and H. Schaffers, "Smart Cities and the Future Internet in Europe," *Journal of the Knowledge Economy* 4: 2 (2013) 119–134.

J.H. Lee, R. Phaal and S. Lee, "An Integrated Service-device-technology Roadmap for Smart City Development," *Technological Forecasting and Social Change* 80:2 (2013) 286-306.

R. McCormick, "Hack leaks hundreds of nude celebrity photos," *The Verge* (September 1, 2014) <http://www.theverge.com/2014/9/1/6092089/nude-celebrity-hack> Accessed on April 18, 2017.

T. Merritt, "Top 5 ways wireless will win," *TechRepublic* (March 27, 2017) <http://www.techrepublic.com/article/video-top-5-ways-wireless-will-win/?ftag=TRE684d531&bhid=27278421562336614541730716262481> Accessed on March 29, 2017.

T. Nam, and T.A. Pardo, "Conceptualizing Smart City with Dimensions of Technology, People, and Institutions," Proc. 12th Conference on Digital Government Research, College Park, MD, (June 12– 15, 2011).

A. Newcomb, "Study Reveals the Age, Nationality and Motivations of Hackers," *NBC News* (September 13, 2016) < http://www.nbcnews.com/tech/security/study-reveals-age-nationality-motivation-hackers-n647171> Accessed on April 12, 2017.

T. Newcombe, "The Rise of the Sensor-based Smart City," *GovTech* (June 2, 2014) <http://www.govtech.com/data/The-Rise-of-the-Sensor-Based-City.html> Accessed on May 2, 2017.

Palo Alto Networks, "Securely Enabling Cloud Adoption," (October 2016) <https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/secure-cloud-adoption> Accessed on January 5, 2017.

D. Reinsel, J. Gantz and J. Rydning, "Data Age 2025: The Evolution of Data to Life-Critical – Don't Focus on Big Data; Focus on the Data That's Big," IDC White Paper (March 2017) < http://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf> Accessed on April 11, 2017.

P. Shakarian, J. Shakarian and A. Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (MA: Elsevier) 2013.

J.M. Shapiro, "Smart Cities: Quality of Life, Productivity, and the Growth Effects of Human Capital," *Review of Economics & Statistics* 88: 2 (2006) 324–335.

D. Shinder, "Understanding and selecting authentication methods," *TechRepublic* (August 28, 2001) < http://www.techrepublic.com/article/understanding-and-selecting-authentication-methods/> Accessed on April 17, 2017.

S.T. Shwayri, "A Model Korean Ubiquitous Eco-City? The Politics of Making Songdo," *Journal of Urban Technology* 20: 1 (2013) 39–55.

F. Siddiqui, "Can hackers take over traffic lights," *The Washington Post* (August 8, 2015) <https://www.washingtonpost.com/local/could-a-hacker-gain-control-of-dcs-traffic-system/2015/08/08/7cb7cf94-201a-11e5-bf41-c23f5d3face1_story.html?utm_term=.28815bd2ec07> Accessed on January 30, 2017.

A. Stratigea, C.A. Papadopoulou and M. Panagiotopoulou, "Tools and Technologies for Planning the Development of Smart Cities," *Journal of Urban Technology*, 22:2 (2015) 43-62.

M. Tomitsch and M.H. Haeusler, "Infostructures: Towards a Complementary Approach for Solving Urban Challenges through Digital Technologies," *Journal of Urban Technology*, 22:3 (2015) 37-53.

A. Townsend, *Smart Cities: Big Data, Civic Hackers and the Quest for a New Utopia* (New York: W.W Norton & Company, 2014).

A. Tanner, "Here's how others can easily snoop on your cellphone," *Forbes* (February 18, 2014) <http://www.forbes.com/sites/adamtanner/2014/02/18/heres-how-others-can-easily-snoop-on-your-cell-phone/#5f6e4566cd33> Accessed on Oct 31, 2016.

A. Vanolo, "Smartmentality: the smart city as disciplinary strategy," *Urban Studies*, 51:5 (2015) 883-898.

J. Viitanen, P. Connell and M. Tommis, "Creating Smart Neighborhoods: Insights from Two LowCarbon Communities in Sheffield and Leeds, United Kingdom," *Journal of Urban Technology*, 22:2 (2015) 19-41.

P. Wang, K.M. Chao, C.C. Lo and Y.S. Wang, "Using ontologies to perform threat analysis and develop defensive strategies for mobile security," *Information Technology Management*, 18 (2017) 1-25.

D. Washburn, U. Sindhu, S. Balaouras, R.A. Dines, N.M. Hayes, and L.E. Nelson, *Helping CIOs Understand "Smart City" Initiatives: Defining the Smart City, Its Drivers, and the Role of the CIO* (Cambridge, MA: Forrester Research) 2010.

D. West, "Achieving Security for Resource-Constrained Devices," *Sensors* (March 17, 2017) < http://www.sensorsmag.com/components/achieving-security-for-resource-constrained-sensors> Accessed on April 18, 2017.

C. Zegras, E. Eros, K. Butts, E. Resor, S. Kennedy, A. Ching and M. Mamum, "Tracing a path to knowledge? Indicative user impacts of introducing a public transport map in Dhaka, Bangladesh," *Cambridge Journal of Regions, Economy and Society*, 8 (2015) 113–129.

K. Zetter, "An Unprecedented Look at Stuxnet, The World's First Digital Weapon," *WIRED* (November 3, 2014) <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/> Accessed on November 17, 2016.

K. Zetter, "Hacking Wireless Printers with Phones on Drones," *WIRED* (October 5, 2015) <https://www.wired.com/2015/10/drones-robot-vacuums-can-spy-office-printer/> Accessed on November 17, 2016.

K. Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *WIRED* (March 3, 2016) <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> Accessed on January 12, 2017.