ANALYSIS

Designing Digital Safety into the Smart City

ROBERT MUGGAH
PRINCIPAL, SECDEV GROUP;
CO-FOUNDER, IGARAPÉ INSTITUTE

All cities face digital opportunities and threats. From the wealthiest to the poorest, urban infrastructure, networks, and citizens are vulnerable to foreign and domestic cyber infiltration. Cities are increasingly at risk (Muggah & Goodman, 2019) as digital services expand and more and more devices are connected to the cloud. City residents are also vulnerable to smart city technologies that can be and are being used to conduct mass surveillance and curb their rights both online and off. If lacking adequate oversight and accountability, the hardware and software of digital cities can unfairly discriminate against minorities.

This article explores two basic questions: (1) What are the cyberthreats facing cities and their residents; and (2) How can cities and city networks work to improve their digital safety? These may be among the most significant – if under-appreciated – questions facing cities in the 21st century. Part of the reason is that most of the world's population is living in cities. The explosive expansion of smart technologies in mature and emerging cities will redefine virtually every aspect of political, economic, and social life. Yet most city leaders and urban residents are only dimly aware of how big the risks are, much less how to deal with them.

The explosive expansion of smart technologies in mature and emerging cities will redefine virtually every aspect of political, economic, and social life. Yet most city leaders and urban residents are only dimly aware of how big the risks are, much less how to deal with them.

The world is currently experiencing two huge mega-trends that are dramatically reconfiguring the future of digital safety in cities and outside of them. The first is the exponential acceleration of technology development and deployment around the world. The global smart city market is expected to grow to over $717 billion by 2023 (Markets and Markets, 2019). The second mega-trend is hyper-urbanisation and the growing concentration of power in cities. More than three million people are moving to cities every week, and by 2050 they will be home to over two thirds of the world's population. These trends are baked in. In the process, cities and city networks are beginning to rival nation states in power and influence (Muggah, 2020).

Technology transformation is occurring so fast – and across so many domains – that it is difficult for international, national, and municipal leaders and institutions to keep up. Indeed, cities around the world are experiencing (or are about to experience) quantitative shifts in IoT, 5G, AI, AR deployment that will transform how metropolitan areas are governed, deliver services, manage commercial exchange, and ensure the safety and security of citizens. Cities are the laboratories, with coalitions of private sector and academic-based institutions driving the process. Along the way, large consultancy firms are overstating many of the upsides of new technologies and downplaying the latent and future risks.

More than three million people are moving to cities every week, and by 2050 they will be home to over two thirds of the world's population.

Meanwhile, turbo-urbanisation has accelerated over the last 50 years. In the 1950s there were just 3 megacities with populations over 10 million people: today there are almost 40. Mega-regions and large metropolitan areas are growth poles in the real and digital economies. Another 2.5 billion people are going to move to cities in the next three decades, albeit most of them in middle- and low-income settings. According to the UN, this is the largest and fastest demographic shift in history. Most of this growth (90%) will occur in Africa and Asia where cities will need to be redesigned, upgraded, or built from scratch. We're seeing an explosion of "smart cities" and "techno hubs": shiny, and often empty, cities in the sands.

These two trends – exponential urban technology expansion and massive urbanisation – are converging. A growing numbers of cities – especially but not exclusively in middle- and upper-income countries – are harnessing new technologies

(remote sensor systems, big data analytics, facial and biometric surveillance) with mixed effects. In some cases, they are developing what I call "agile security" solutions (Muggah, 2018). To be sure, all cities are on the way to becoming digital cities albeit at different temporal and spatial scales. The rules and regulations to manage these processes are evolving haphazardly, even as data protection groups are weighing in. Some cities like San Francisco and Oakland are banning certain technologies (O'Brien, 2019) like facial recognition (many more are using them – D'Onfro, 2019), while others such as those in China are doubling down on mass surveillance (Keegan, 2019).

So what are the big risks that cities are facing in the short-term? There are at least three big clusters: (1) cyberattacks, (2) mass surveillance, and (3) algorithmic bias and discrimination. I'll very briefly focus on these before turning to possible solutions.

The first major threat to making cities "digitally safe" is attack from external and domestic sources. We are already seeing a major escalation of cyberattacks – ransomware, phishing, DDOS attacks, kill-disk malware – targeting municipalities around the world (Muggah & Goodman, 2019). Most of the tools are off-the-shelf and sourced from the Deep Web. Think of them as the 21st-century automatic weapon – cheap, easy to use, and running 24/7. The increases in attacks globally are alarming. About 70% of all reported ransomware attacks in the U.S. in 2018 (Freed, 2019) targeted critical infrastructure – hospitals, schools, police, emergency hotlines, and businesses in counties and cities. At least 70 state and local governments were attacked involving over 620 digital extortion incidents in 2019 (Fernandez, Sanger, & Martinez, 2019 and Ng, 2019). The truth is no one knows how big these challenges really are – cities and insurance companies are reluctant to disclose details. Most cities cannot even tell if their IT systems are subject to breaches.

About 70% of all reported ransomware attacks in the U.S. in 2018 targeted critical infrastructure – hospitals, schools, police, emergency hotlines, and businesses in counties and cities.

An epidemic of cyber threats facing cities are global. London was hit by almost 1 million attacks a month in 2019 according to Centrify's Freedom of Information request (Narendra, 2019). Ransomware jammed municipal trams in Dublin (Ms. Smith, 2019) and railway ticketing in Stockholm (Johnson, 2017) in recent years. City power plants were also targeted from Hyderabad (Pradhan, 2019) to Johannesburg (BBC, 2019) over the past year. Kiev has become a testing site or even a battleground for all manner of cyber malfeasance, drawing state intelligence units, state-sponsored advanced action groups, and various types of white and black hat hackers (Greenberg, 2017). The costs of these digital incursions are soaring. It is not just the costs of extortion, but the knock-on effects of repairing systems, lost productivity, and rising insurance premiums that are over-burdening local governments. Cities are being targeted because they are soft targets – awareness is low, systems are outdated, and skills are limited.

The truth is that cities globally are poised at the very beginning of a dangerous cyberattack escalation. The coming digital economy and expanding automation of the public and private sectors are a nightmare for cities. Metropolises will soon be managing hundreds of billions of hackable, unpatchable, and unupgradable devices connected to subnational, national, and international grids. So far, most cyberattacks have targeted urban legacy infrastructure, including systems that are either forgotten or poorly managed by IT departments. It is useful to recall that despite the hype, most cities are still generally "dumb". The real concern is what happens when the attack surface increases dramatically and oil production, electricity grids, transportation systems, water supplies, and all manner of basic services that citizens depend on are exposed?

The second big obstacle to digital safety is mass surveillance. The rising capacity for surveillance is an intrinsic property of "smart cities" – data collection technologies and systems are used for everything from traffic lights and parking to energy use, water management, and policing. Indeed, there has been a sharp rise in the deployment of connected cameras, facial recognition, biometric and scanning systems at the borders of – and across – cities.

But when such technologies are persistent, unaccountable, exploited, and unidirectional, they raise legitimate questions about citizen safety and civil liberties both online and off. Some analysts fear that smart cities themselves are a crucible of "panopticon" society where surveillance is mediated by selective biases of its operators.

Metropolises will soon be managing hundreds of billions of hackable, unpatchable, and unupgradable devices connected to subnational, national, and international grids.

Predictably, there are of course some parts of the world where mass surveillance in cities is more intensive than in others. For example, authoritarian and autocratic systems tend to be early adopters of surveillance technologies. Roughly 8 out of the 10 most heavily monitored cities in the world (Zhang, 2019) are in China (the others are Atlanta and London). The city of Chongqing has 2.6 million cameras – one for every six residents – beating out even Beijing, Shanghai, and Shenzhen. There we see a combination of "sharp eyes" monitoring (AI-enabled facial, gait, and biometric surveillance; Denyer, 2018) and the infamous "social credit score" (Marr, 2019). Whether made in China, Israel, or the US, similar technologies are being exported around the world.

While government surveillance in democratic and non-democratic societies is typically cast as a desire to "protect citizens", this is not always welcomed by local residents. Indeed, there are obvious ways that intrusive technologies can reduce people's sense of autonomy or privacy and undermine their digital safety. For one, even when surveillance is anonymised, it can reveal "personally identifiable information" that may be protected by privacy laws. The overly broad application of certain technologies (like biometric surveillance) without a "pressing social need" may even violate the International Covenant on Civil and Political Rights. These concerns are voiced more prominently in Western European and North American constituencies than elsewhere.

A third and related challenge involves biases and discrimination in urban digital hardware, software, and their application. As machine learning tools and data-driven software play an increasingly important role in how city governments make decisions, the concerns with how these algorithms are designed and used keep rising. There are real and justified concerns that using data stained with prejudiced policing, judicial practices, or (potentially unconscious) biases of developers will discriminate against minorities and others (Aguirre, Badran, & Muggah, 2019, p. 8–9). Some technology companies recognise the risks that such tools generate (not least to their bottom line), but as noted above, these tend to be downplayed.

While government surveillance in democratic and non-democratic societies is typically cast as a desire to "protect citizens", this is not always welcomed by local residents. Indeed, there are obvious ways that intrusive technologies can reduce people's sense of autonomy or privacy and undermine their digital safety.

While the digital challenges facing cities are real, there are also unexpected opportunities. Indeed, the dizzying spread and lowering costs of new technologies mean that fast-growing cities in Africa and Asia may have the second-mover advantage (Aggarwala, Hill, & Muggah, 2018). If urban leaders, planners, and developers take the right decisions early as cities are being designed and developed, they can potentially avoid making the mistakes of their counterparts in other parts of the world. These cities can be designed with digital safety and security in mind from the beginning, not mid-way through or at the end of the process. They will also have tremendous opportunities to leap-frog legacy systems and adopt more efficient options.

If urban leaders, planners, and developers take the right decisions early as cities are being designed and developed, they can potentially avoid making the mistakes of their counterparts in other parts of the world.

First, cities need to adopt a digital safety mindset. A smart city is a digitally secure city. This means having plans, protocols, and personnel in place before, during, and after attacks occur. It means having the right intelligence-led systems in place to detect, mitigate, and contain threats before they spread and having cyber risk insurance in place for when cities are hit, as they surely will be. It means reducing attack surfaces in the city and segmenting networks so that a single point of entry doesn't end up bringing down the entire system. It also requires ensuring city intelligence is informed by the wants and needs of citizens, and not just ICTs.

Second, city executives need to assume a leadership role in digital safety and security. Just like we have mayors coming out in defence of climate and migration, we need our top officials championing digital safety. This is important. Most technology experts say that city mayors and managers don't take cyber security seriously enough. Our mayors, city managers, CIOs, CTOs, and utility executives need to work with partners across society to adopt a whole-of-city approach aligned with the smart city strategy. Building a "joint venture" approach can reduce the likelihood of adversarial relationships between governments and city residents.

Third, cities need to recruit the right personnel to adapt to fast-changing challenges. This means attracting the right talent – including engineers, coders, and hackers. Cities can also outsource some of their needs – some are even issuing RFPs to hire ethical hackers to test city networks and assets. This isn't easy for cities with shrinking budgets and ballooning deficits. But recruitment, together with regular training for all city staff and associated service providers is key. It's often the most basic human errors that cause the biggest problems. Sometimes it's just the simplest of patches – software upgrades, up-to-date firewalls, frequent backups, and multi-factor authentication – that make all the difference.

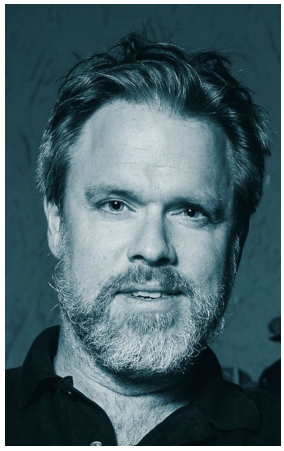
Fourth, cities should more actively incubate digital safety solutions. Of course the legal frameworks at the international, national, and state levels matter – but cities have more discretion than they often realise. Cities can crowd-source and help nurture solutions from the global to the municipal scale. For example, they can create open data portals – as many have done – to allow researchers and residents to build apps to improve safety. They can accelerate innovation through incentive competitions or bug bounties. This is a win-win for cities, since by building local innovation ecosystems they also reduce reliance on outside vendors.

Fifth, cities should increase citizen involvement in decision-making and design processes involving digital safety. This is critical, since citizens are increasingly rejecting technologies that are seen as intrusive and opaque. One way to build awareness is through what researchers call the "triple helix" – the combined efforts of government, business, and universities working together. Activities such as smart citizen labs and ICT tasters can help spread understanding and optimise residential uptake of new innovations.

Sixth, cities may wish to set out guidance or standards for algorithmic transparency in decision-making platforms used by the government and related service providers. While the legal case will vary from jurisdiction to jurisdiction, cities could explore ways to improve the explainability, responsibility, accuracy, auditability, fairness, and privacy of their key technologies impinging on safety and security (especially as it relates to, say, issues of crime control, criminal justice and probation, provision of public and financial services).

Finally, cities need to initiate a conversation about the necessary national and global rules and standards to improve digital safety. They cannot wait for nation states or international organisations to take the lead, nor can they rely on business to save them. To do this, urban centres and citizens need to be digitally literate and practice good digital hygiene. Some cities and states are also experimenting with legislation to require all tech devices to have reasonable security features that prevent unauthorised access, modification, and information disclosure. Such norms are more effective if city residents are part of the process of developing such laws to begin with.

Ensuring cities are digitally safe and secure is a comprehensive and complex agenda. But the truth is that the seven priorities identified above are the minimum that must be done. City governments, public utilities, service providing agencies, commercial entities, and digital rights groups will need to learn from one another, share experiences, and start thinking about more agile norm setting. They will need to be pressing governments and intergovernmental bodies to take bolder action. After all, cities are bearing the brunt of digital insecurity. And the situation is about to get a whole lot worse before (if) it gets better. ■



About the author:

Robert Muggah is a globally recognized specialist in cities, security and new technologies. He is a principal of the SecDev Group – a digital risk consultancy working at the interface of the digital economy and urbanization. At SecDev Group, Muggah helps city, corporate and non-profit leaders improve their future preparedness through high resolution data-driven diagnostics, strategy development, exponential leadership training, and public talks. In addition to his work at SecDev, he is also research director of the Igarapé Institute - a think and do tank - known for developing award-winning data visualizations and technology platforms to improve public safety.

Muggah has spend decades tracking past and future trends in urban risk. He is faculty at Singularity University, senior adviser to McKinsey and Company, a fellow and adviser to the World Economic Forum, chair of the Global Parliament of Mayors, and a regular consult to the United Nations and World Bank. Muggah is the author of seven books and hundreds of peer-review and policy-oriented studies, including Impact: Maps to Navigate our Past and Future (Penguin, with Ian Goldin, out in 2020). His research is featured in global media, including the BBC, CNN, Economist, Financial Times, Guardian, New York Times, USA Today and Wired. He has given several TED talks viewed by millions, and speaks regularly at the Davos Summit. Muggah received his DPhil from the University of Oxford and his MPhil from the University of Sussex.

References

Aggarwala, R. T., Hill, K., & Muggah, R. (October 2018). Smart city experts should be looking to emerging markets. Here's why. Retrieved from https://www.weforum.org/agenda/2018/10/how-the-developing-world-can-kickstart-the-smart-cities-revolution/

Aguirre, K., Badran, E., & Muggah, R. (July 2019). *Future Crime: Assessing twenty first century crime prediction.* Retrieved from https://igarape.org.br/wp-content/uploads/2019/07/2019-07-12-NE_33_Future_Crime.pdf

BBC. (July 2019). Ransomware hits Johannesburg electricity supply. Retrieved from https://www.bbc.com/news/technology-49125853

D'Onfro, J. (July 2019). This Map Shows Which Cities Are Using Facial Recognition Technology—And Which Have Banned It. *Forbes*. Retrieved from https://www.forbes.com/sites/jilliandonfro/2019/07/18/map-of-facial-recognition-use-resistance-fight-for-the-future/

Denyer, S. (January 2018). China's watchful eye. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/

Fernandez, M., Sanger, D. E., & Martinez, M. T. (August 2019). Ransomware Attacks Are Testing Resolve of Cities Across America. *The New York Times.* Retrieved from https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html

Freed, B. (August 2019). Report: Two-thirds of ransomware attacks in 2019 targeted state and local governments. Retrieved from https://statescoop.com/report-70-percent-of-ransomware-attacks-in-2019-hit-state-and-local-governments/

Greenberg, A. (June 2017). How an Entire Nation Became Russia's Test Lab for Cyberwar. Retrieved from https://www.wired.com/story/russian-hackers-attack-ukraine/

Johnson, S. (May 2017). Swedish local authority says hit by cyber attack. Retrieved from https://www.reuters.com/article/us-britain-security-hospital-sweden/swedish-local-authority-says-hit-by-cyber-attack-idUSKBN1882OI

Keegan, M. (December 2019). Big Brother is watching: Chinese city with 2.6m cameras is world's most heavily surveilled. *The Guardian*. Retrieved from https://www.theguardian.com/cities/2019/dec/02/big-brother-is-watching-chinese-city-with-26m-cameras-is-worlds-most-heavily-surveilled

Markets and Markets. (2019). *Smart Cities Market by Smart Transportation, Smart Buildings, Smart Utilities, Smart Citizen Services, and Region* [TC 3071]. Retrieved from https://www.marketsandmarkets.com/Market-Reports/smart-cities-market-542.html

Marr, B. (January 2019). Chinese Social Credit Score: Utopian Big Data Bliss Or Black Mirror On Steroids?. *Forbes*. Retrieved from https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/

Ms. Smith. (January 2019). Hacker posts ransom demand on Dublin's Luas tram system site. Retrieved from https://www.csoonline.com/article/3330651/hacker-posts-ransom-demand-on-dublins-luas-tram-system-site.html

Muggah, R. (June 2018). How smart tech helps cities fight terrorism and crime. Retrieved from https://www.weforum.org/agenda/2018/06/cities-crime-data-agile-security-robert-muggah/

Muggah, R. (January 2020). Look to cities, not nation-states, to solve our biggest challenges. Retrieved from https://www.weforum.org/agenda/2020/01/cities-mayors-not-nation-states-challenges-climate/

Muggah, R., & Goodman, M. (September 2019). Cities are easy prey for cybercriminals. Here's how they can fight back. Retrieved from https://www.weforum.org/agenda/2019/09/our-cities-are-increasingly-vulnerable-to-cyberattacks-heres-how-they-can-fight-back/

Narendra, M. (August 2019). #privacy: City of London hit by nearly one million cyber-attacks each month. *PrivSec Report*. Retrieved from https://gdpr.report/news/2019/08/23/privacy-city-of-london-hit-by-nearly-one-million-cyber-attacks-each-month/

Ng, A. (December 2019) Ransomware froze more cities in 2019. Next year is a toss-up. Retrieved from https://www.cnet.com/news/ransomware-devastated-cities-in-2019-officials-hope-to-stop-a-repeat-in-2020/

O'Brien, M. (December 2019). Why some cities and states ban facial recognition technology. *The Christian Science Monitor*. Retrieved from https://www.csmonitor.com/Technology/2019/1218/Why-some-cities-and-states-ban-facial-recognition-technology

Pradhan, S. D. (November 2019). Cyber-attack on Kudankulum Nuclear Power Plant underlines the need for cyber deterrent strategy. *The Times of India*. Retrieved from https://timesofindia.indiatimes.com/blogs/ChanakyaCode/cyber-attack-on-kudankulum-nuclear-power-plant-underlines-the-need-for-cyber-deterrent-strategy/

Zhang, P. (August 2019). Cities in China most monitored in the world, report finds. *South China Morning Post*. Retrieved from https://www.scmp.com/news/china/society/article/3023455/report-finds-cities-china-most-monitored-world