



Smart and Safe

Risk Reduction in Tomorrow's Cities

Smart and Safe: Risk Reduction in Tomorrow's Cities

Executive Summary	4
1 Introduction	9
2 How to Use this Guide	12
3 What's New about Risk in the Smart City?	18
4 Responding to the City-wide Challenges	24
4.1 Cybersecurity: Connect Smart	26
4.2 Cyber Resilience: Fail Safe	30
4.3 Privacy and Data Protection: Manage Responsibly	32
4.4 Collaboration and Coordination in Governance: Govern Inclusively	36
5 Creating a Roadmap Towards a Secure and Resilient City	38
6 Conclusion	40
7 Appendix – Defining Key Terms: Smart Technologies	42





In land-scarce **Singapore**, twelve percent of land is set aside for roads and transport infrastructure. The city is implementing an ambitious Smart Nation strategy, pursuing innovations such as wearables that act as payment devices for public transit, autonomous buses and on-demand shuttles. Public data sets and data analytics are available to the public and third party developers. (smartnation.sg)



Executive Summary

A city's leadership holds paramount responsibility for securing Smart Cities. This Guide identifies challenges and provides recommended actions in four key domains: cybersecurity, cyber resilience, privacy and data protection, and collaboration and coordination in governance.

Transform Cities Through Smart Technology, Emphasizing Security and Safety

Increased urban populations, climate change, political and management complexity and resource scarcity challenge today's city executives. Cities around the globe are investing in Smart City initiatives and technology to improve efficiency, resilience and quality of life for their residents. Thoughtfully applied, smart technology can make cities more livable and attractive, increase safety and security, and enhance resident participation. Smart Cities offer a wealth of possibilities by transforming how a city's services—including transportation, power, water and communications—are delivered. However, the new technologies also pose critical risks to safety, security and to vital city functions, risks that often remain underestimated.

This Guide is designed to provide **guidance for Smart City executives** on making a Smart City secure and safe by managing technology effectively. The transformation must bring together all parties—community members, businesses, civic and religious organizations, non-governmental organizations and charities, municipalities, and governments—to combine efforts to this end.

A city's leadership holds paramount responsibility for securing Smart Cities. This Guide **identifies challenges and provides recommended actions in four key domains: cybersecurity, cyber resilience, privacy and data protection, and collaboration and coordination in governance.**



What is a Smart City?

The United Nations defines a Smart and Sustainable City as “an innovative city that uses information and communications technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social, environmental as well as cultural aspects.”

Source: ITU-T Study Group 5, (2015). <https://www.itu.int/en/ITU-T/focusgroups/ssc/Pages/default.aspx>

The European Union Agency for Network and Information Security (ENISA) defines a Smart City along two common integral elements: (1) basic processes that characterize Smart Cities, such as the extensive use of ICT in general or the application of big data analytics in particular to meet public needs; and (2) specific focus areas attached to (enabled by) these processes, such as improving mobility or resilience, or addressing environmental challenges.

Source: ENISA (2016). Architecture model of the transport sector in Smart Cities. January 12. <https://www.enisa.europa.eu/publications/smart-cities-architecture-model>

Manage Emerging Risk

Increased reliance on technology can increase risk. Three technology attributes are essential to the benefits of Smart Cities but also increase risk:

- **Scale and Speed:** the enormous number of smart devices rapidly deployed by multiple players;
- **Interconnection:** the unstructured networks that connect these devices are networked to each other and to critical infrastructures, creating complex interdependencies across services; and
- **Novelty:** the adoption of radically innovative technologies and capabilities.

Respond to City-wide Challenges

These technology attributes lead to three, closely interrelated, city-wide challenges. These include:

- Expanded **Operational Risk**;
- Increased **Management Complexity**; and
- New Levels of **Uncertainty and Distrust**.

Uncertainty and distrust exacerbate operational

risk and management complexity; at the same time, unmanaged operational risk fuels uncertainty and distrust. Responding to these challenges requires continuous attention and strategic thinking—about people, processes and technology, as well as law and policy.

Focus on Four Domains

Cities must define acceptable risks and implement a risk management framework. They should complement the risk management framework with a tested incident and emergency response plan. These actions and those summarized below will **substantially reduce the downside risk**, help realize the technology's **anticipated benefits** and subsequently, **enhance trustworthiness**, acceptance and adoption of the Smart City by residents and businesses.

1. Cybersecurity: Connect Smart

Cybersecurity is critical to ensure the confidentiality, integrity and availability of systems and information. It requires an integrated approach that prevents, detects and mitigates the effects of incidents or attacks at every potentially vulnerable layer including devices, networks, applications and cloud

platforms. “Connect Smart” involves deciding when and how to connect devices and systems to each other. Key elements include:

a. Buy Secure: Know and enforce key security characteristics through risk-informed procurement, including the capabilities for regular security patching and upgrading; changing default passwords and encrypting communication; strong authentication of people and devices; and security certification of technology.

b. Map and Manage the Networks: Use the network to enforce security, including maintaining an accurate inventory of your ICT environment, network segmentation and incident handling.

c. Practice “Need to Know”: Exercise prudence when deciding to interconnect and run devices and applications. Legitimate data goes only where and when it is intended.

d. Authenticate Access: Every device and online user should be authenticated.

2. Cyber Resilience: Fail Safe

Cyber resilience ensures the ability of a city's complex cyber systems to continuously deliver critical outcomes despite everyday glitches and acute shocks; it requires

strong cybersecurity. By “failing safe,” a Smart City can adapt and recover while still delivering public safety and other critical services according to predetermined levels. Key elements include:

a. Ensure Redundancy:

Identify central operational components where non-availability would have immediate, significant consequences, and build in redundant infrastructure and alternative approaches on a technical and organizational level.

b. Design-in Safety

Defaults: Systems, devices and networks should reboot or restart in a safe configuration to provide basic services until the situation is restored.

c. Test-Exercise-Adjust:

Ensure resilience through periodic testing of scenarios, city-wide disaster exercises, and adjusting plans, procedures, devices, systems and networks.

3. Privacy and Data Protection: Manage Responsibly

To protect data (and ensure the public’s trust), Smart Cities must manage data responsibly through technical and organizational measures. At a minimum, this includes following widely accepted, basic privacy and data protection principles. Additional elements include:

a. Proclaim a Privacy and Data Protection Charter:

Enshrine principled privacy-by-design and privacy-by-default approaches in the overall Smart City operations and champion privacy-preserving technologies and technical and organizational best practices.

b. Enhance Transparency and Appoint a Chief Privacy Officer:

Prescribe regular public reporting on the state of privacy and data protection and conduct privacy impact assessments for critical domains. Task a senior role to oversee privacy and data protection.

c. Require Data Governance Agreements with Third Parties:

Define clearly the type, usage and ownership of sensitive data processed by third parties.

4. Collaboration and Coordination in Governance: Govern Inclusively

Organizational structures, mechanisms, and incentives are crucial for overall Smart City efforts. Cybersecurity, resilience and privacy are key to these structures and mechanisms to ensure coherence of shared values for effective and efficient collaboration and coordination. Key elements include:

a. Deploy Collaboration and Coordination Platforms:

Employ digital forums and tools to strengthen collaboration and coordination and

enable crowdsourced solutions from diverse groups of stakeholders.

b. Organize for Engagement:

Lead engagement within the city and those who depend on its services to manage issues across domains and beyond the city’s borders.

c. Communicate Clearly and Often:

Decisions ultimately reflect hard trade-offs regarding security, privacy and budget priorities. Clear messaging about decisions and their rationale will build trust and inclusivity.

Define a Roadmap

Implementing security and resilience into a Smart City is a complex undertaking and must be spearheaded by senior city executives. A roadmap incorporates the Smart City’s vision and values and determines goals, strategies and actions that ensure security, resilience and privacy. It also establishes structures and processes for effective governance. The roadmap should (1) identify a Smart City vision; (2) ensure broad stakeholder participation; (3) map critical risk and interdependencies; (4) mitigate risk and ensure benefit realization; (5) define adequate levels of security and resilience; (6) adapt governance structures; and (7) ensure informed investment decisions.



Decidim.Barcelona, a digital platform for civic participation, offers users a way to take part in **Barcelona** city council decisions. An open software approach allows any citizen to see how the platform is built, reuse the code, and make suggestions for improvements. (www.decidim.barcelona)



1 Introduction

Thoughtfully applied, technology makes cities smarter. Urban populations will rely on government leaders to take advantage of technology to improve city operations and enhance urban livability and attractiveness, increase safety and security, and strengthen resident participation.

Today, cities are home to three-quarters of the earth's population. In these spaces, emergent smart technologies are transforming our work and our lives. The data collected by millions of devices and the applications that harness it create high visibility into urban activities and new opportunities that reshape, and even revolutionize those activities, (e.g., the experiences of traditional taxi companies and traffic planners with the emergence of ride share apps). The forces of urban transformation unleashed by the wide deployment of smart technologies will continue to produce social and economic benefits as well as disruptions. Cities must manage these changes in urban life, mitigating negative consequences while capturing the benefits.

The technological transformation in the urban environment began with the digitalization of government and municipal services, enabling businesses, residents and city administrators to request and deliver public services more efficiently via the Internet. Opening large caches of data to the public (and to other city agencies) will further stimulate new services and improve decision-making. City operations (e.g., water, power, transit) can benefit from networked sensors and actuators.

By 2020, some 25 billion devices will be connected to the Internet; commonly referred to as the Internet of Things (IoT).¹ The number of Smart Cities is expected to rise fourfold by 2025, with significant investments in technologies and high expectations on return.²

Thoughtfully applied, technology makes cities smarter. Urban populations will rely on government leaders to take advantage of technology to improve city operations and enhance urban livability and attractiveness, increase safety and security, and strengthen resident participation.

¹ Amy Nordrum (2016). Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. IEEE Spectrum. <https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated>.

² Smart Cities to Rise Fourfold in Number from 2013 to 2025, <https://technology.ihs.com/507030/smart-cities-to-rise-fourfold-in-number-from-2013-to-2025>; Smart Cities - Statistics & Facts. <https://www.statista.com/topics/4448/smart-city>.

New Opportunities ...

Smart Cities already offer a wealth of possibilities and will continue to do so as technology and applications evolve. Complex, diverse networks connect transportation, power, water, communications infrastructures and other utilities with associated business and management systems. Interconnecting the digital and physical worlds, smart technologies enable new forms of public service delivery and management. While sensors play an important role, what really makes a city smart is the analytics that turn collected data into usable, actionable information. Thus, the use of big data and data science—supported by machine learning and artificial intelligence (AI)—will be critical technological components of Smart Cities.

For example, in the transportation sector, the advent of IoT and data analytics means that taxis,

buses and traffic monitors can be networked and tracked to enhance convenience and predictability. Importantly, these local solutions can have larger impacts: more efficient transportation systems can improve mobility and safety while reducing energy consumption, commuter time and environmental impact. (See page 15.)

Smart must also mean safe. With focus and guidance, the same technologies can also reduce pedestrian fatalities as well as enhance public safety, increasing public confidence that police, fire, emergency medical services and hospitals are equipped with important data that can help them prevent, detect and respond to incidents.³ Smarter, safer cities

³ The Guide uses “public safety” to include emergency services such as police, fire and emergency medical services and it uses the terms “safety and security” or “safety and security for the public” to describe the more abstract good of safety and security in a community.

address the growing public demand that officials do more than merely react to problems. Smart Cities can pinpoint potential problems before they reach a critical point to protect people and communities from harm. For instance, networked sensors can monitor traffic-related infrastructure—such as structural integrity of tunnels or bridges and air—boosting safety, security and public health.⁴ That is smart, and it is also safe. (See page 16.)

Finally, Smart Cities have the potential to enhance individuals’ sense of place and belonging. Community apps and platforms can foster connections among neighbors and assist families, children and seniors by expanding their independence and safety.

⁴ Leon Erlanger (2016). State and Local Governments Embrace IoT, Including in Smart Cities. <https://statetechmagazine.com/article/2016/07/state-and-local-governments-embrace-iot-including-smart-cities>.



...and New Risks

However, critical security, safety and privacy risks remain underestimated. For instance, we must pay greater attention to how Smart Cities deliver on their promises while not becoming the victims, or the unwitting facilitators, of cyber crimes. To date, conventional approaches to critical infrastructure protection and interconnected physical and digital systems in cities have:

- Focused on individual sectors or domains (e.g., energy, communications, transportation) rather than taking a comprehensive approach. Physical-cyber interactions, cascading effects and systemic risk have not been factored sufficiently into policy, planning and operations;⁵
- Faced novel political and regulatory conflicts as unexpected consequences

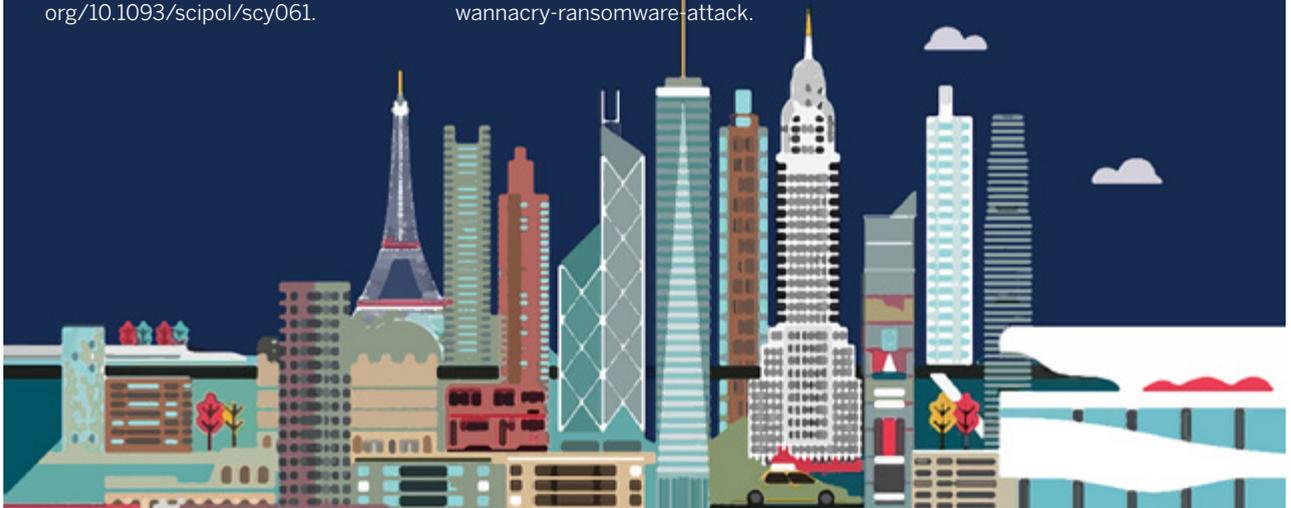
⁵ Aaron Clark-Ginsberg and Rebecca Slayton (2018). Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards. *Science and Public Policy*, <https://doi.org/10.1093/scipol/scy061>.

of disruptive innovation (e.g., increased congestion and the displacement of traditional taxis, dangers associated with AI-enabled self-driving cars);

- Exacerbated societal inequalities and disenfranchised individuals instead of creating new opportunities, fueling economic growth and improving quality of life;
- Magnified technology risk and introduced new vulnerabilities that could lead to cascading failures across multiple infrastructures within and beyond a single city; and
- Attracted the interest of malicious actors including trusted insiders who use cyber attacks to target smart infrastructure causing damage, stealing information for financial gain or disrupting critical services.⁶

⁶ For example, the 2017 WannaCry ransomware attack that crippled, among others, health and emergency services and hospital systems in the United Kingdom and spread around the globe. See, Symantec (2017). What you need to know about the WannaCry Ransomware. Symantec Security Response, May 23. <https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack>.

To fully enjoy the benefits of deploying IoT and smart, networked technologies, cities must address security and privacy in both the digital and physical realms to mitigate potential harms ranging from the disruption of essential services to machine-generated bias in service delivery. The process of transformation must bring together all parties—community members, businesses, civic and religious organizations, non-governmental organizations and charities, municipalities and governments—to collaborate and coordinate efforts. As the private sector owns or operates most systems and critical infrastructure, meaningful public-private partnership is critical. Cities have much to gain and lose; they must anticipate and manage new risks, many of which extend beyond the technical and operational dimensions. This Guide is designed to help.



2 How to Use this Guide

This Guide focuses on how to make a Smart City secure and safe by managing technology effectively—and smartly. It provides guidance for Smart City managers and executives—an expansive term used in this Guide to describe city leaders and those responsible for Smart City initiatives and city planning.

Regional and national planners, policymakers, technology vendors, commercial builders and developers, and individuals will also learn about **critical security and safety challenges associated with Smart Cities** and how to address them. The recommendations in this Guide underscore the need to integrate and connect existing strategic plans, digital economy strategies, cybersecurity strategies, critical infrastructure protection and resilience plans and technology policy decisions (e.g., regarding spectrum allocation) at every level: not only in the metropolitan area, but also at the state, regional and national levels.

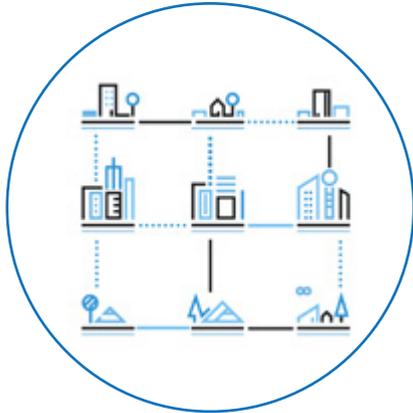
City governments hold paramount leadership responsibility for securing Smart Cities. They should:

- Apply sound risk management and digital security⁷ best practices to their own operations, including through risk-informed purchasing decisions;
- Incentivize the application of sound cybersecurity and privacy practices by all participants in the Smart City ecosystem, including non-governmental providers of essential services; and
- Align digital security efforts with more fundamental objectives to create trust, security and safety in the city.

Without solid digital security, cities that deploy smart technologies will put their operations at serious risk. This Guide sets out to mitigate this risk by **identifying and describing challenges** (section 3) and **providing recommended actions** in four domains (section 4).

⁷ In this Guide, achieving “digital security” requires action across four domains, including (traditional) cybersecurity, cyber resilience, privacy and data protection, and sound governance.

Four Key Domains:



Cybersecurity:

The confidentiality, integrity and availability of cyber-connected systems, infrastructure and related data.



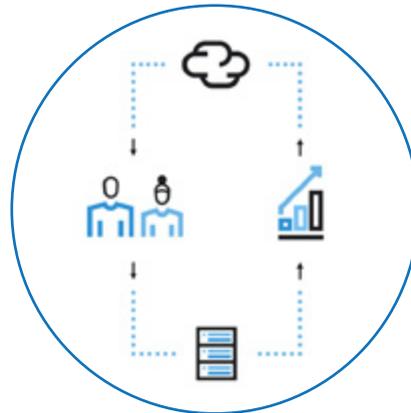
Cyber Resilience:

The ability of a city's complex cyber systems to deliver essential services continuously in the face of acute shocks and disruptions. Cyber resilience requires strong cybersecurity.



Privacy and Data Protection:

The protection of personal data in an increasingly digital world, gaining the trust of users and residents to enable full participation in the Smart City's benefits.



Collaboration and Coordination in Governance:

The effective management structures and incentives for collaboration and coordination with multiple stakeholders.



London is a leader in urban mobility. The Tube carries more than a billion passengers each year, four million journeys each day and growing. Transport for London, the city's transportation authority, is responsible for enacting the Mayor's Transportation Strategy, including driving changes in traffic management, transit networks, and bike sharing. (tfl.gov.uk)





Highlights

Transportation in the Smart City

Transportation should be closely integrated with energy, public safety, environmental monitoring and waste management. **Traffic sensors** that work with navigation applications can steer users away from congestion and road hazards. **Smart traffic signals** can ensure the rapid passage of emergency service vehicles along a given route. Sensor data can be used to identify roads and intersections that are routinely overwhelmed, enabling responses that reduce the likelihood of accidents. London and Singapore are already using smart technology in these ways. In Barcelona **smart lighting** adjusts levels according to weather conditions and time of day. Brightness can be increased in an instant to help emergency personnel respond to a traffic accident at night. Swiss authorities intend to boost rail capacity by up to 30 percent by linking rail transportation systems to advanced **data analytics**. Trains will travel more quickly, more frequently and more safely—all while conserving energy. In addition to increasing efficiency, smart public and private transportation can save energy and improve the safety and security of the public. In the near future, **autonomous vehicles, self-driving trucks** and cars as well as **drones** will create new realities for private and commercial transportation in cities.⁸

⁸ ENISA (2016). Architecture model of the transport sector in Smart Cities. January 12. <https://www.enisa.europa.eu/publications/smart-cities-architecture-model>.



Highlights

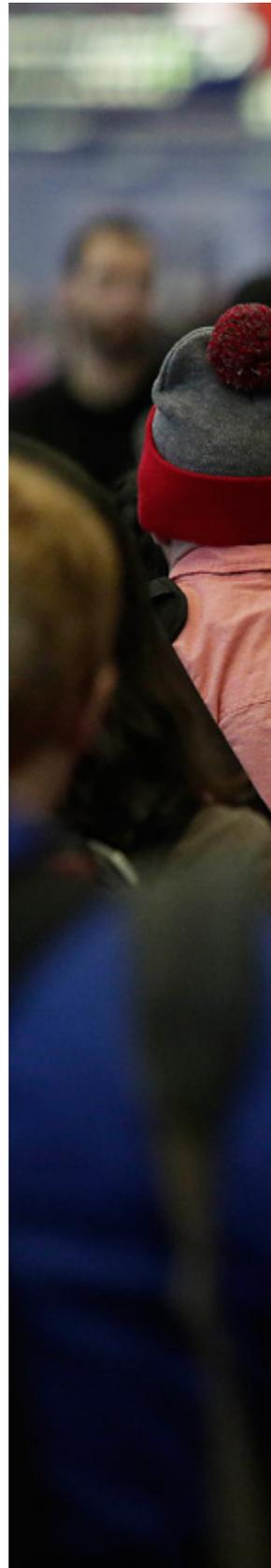
Public Safety in the Smart City

The use of new technologies coupled with intelligent algorithms can complement traditional law enforcement work and help to prevent and investigate crime. **Gunfire detection systems** can inform law enforcement about a crime and reduce response time for them to arrive at a crime scene.⁹ Using a net of acoustic sensors, typically fixed to a light pole, telephone pole or the roof of a building, gunfire detection systems identify the location where a firearm has been discharged by acoustic triangulation and overlay this information on a digital map to determine exact coordinates or address information. Receiving this information in real-time, the police dispatcher can instruct the nearest police vehicle or officers to respond to the scene. Exploiting the powers of computer **algorithms and big data/data science** (based on, for example, “crime data with factors including the location of local businesses, the weather and socioeconomic information to forecast where crime might occur”), law enforcement has been using **predictive policing** to plan police officer deployments in order to prevent crime before it occurs.¹⁰ For example, in Chicago, a 2.7 million person city with a high rate of gun violence, certain areas have seen a significant reduction of crime, “between 15-29 percent fewer shootings, and 9-18 percent fewer homicides.” In one district, the numbers fell even more significantly, with a 39 percent drop in shootings and a decrease of 33 percent in the number of murders over the same period the previous year.¹¹ These tools, when deployed with careful attention to potential disproportionate impacts on low income and minority residents, adequate transparency, community engagement and training for police forces, can contribute to increased public safety throughout a city.

⁹ Juan R. Aguilar (2015). Gunshot Detection Systems in Civilian Law Enforcement. *Journal of the Audio Engineering Society*, 63 (4), pp. 280-291. <https://doi.org/10.17743/jaes.2015.0020>.

¹⁰ Martin Kaste (2018). How Data Analysis Is Driving Policing. NPR, All Things Considered, June 25. <https://www.npr.org/2018/06/25/622715984/how-data-analysis-is-driving-policing>.

¹¹ Timothy McLaughlin (2017). As shootings soar, Chicago police use technology to predict crime. Reuters, August 5. <https://www.reuters.com/article/us-chicago-police-technology/as-shootings-soar-chicago-police-use-technology-to-predict-crime-idUSKBN1AL08P>.





The **Chicago** Police Department has undertaken several technology initiatives to improve policing and community engagement, including establishing Strategic Decision Support Centers in violent areas. These centers use predictive crime software, cameras and gunshot detection systems, to deliver real-time notifications and intelligence to officers in the field. (home.chicagopolice.org)



3 What's New about Risk in the Smart City?

Interconnectivity and integration across virtual and physical infrastructures are essential to making cities smart, yet they are also a source of new vulnerabilities and risks.

The deployment of smart technologies creates new vulnerabilities and modes of failure. While some of these fall into existing, well-understood categories, others may create new categories and pose significant new risk. For instance, AI introduces a nonlinear risk dimension to Smart City technology deployments. This chapter of the Guide provides a framework for understanding how smart technologies lead to city-wide challenges and how Smart City managers can take actions to address them.

Smart Cities are complex, open systems. Millions of IoT devices from different manufacturers interconnect through multiple network infrastructures, interact with cloud platforms, and use artificial intelligence for data analysis, decision-making and automation. Interconnectivity and integration across

virtual and physical infrastructures are essential to making cities smart, yet they are also a source of new vulnerabilities and risks. A single, seemingly innocuous but vulnerable IoT device can spread malware or erroneous data across multiple networks and lead to cascading degradation of essential services. Poorly configured devices can be maliciously repurposed and used for attacks on internal or external networks.¹² Faulty sensors, crashed systems or corrupted data can have severe consequences, such as shutting down access to the fire department, the police or utilities in an emergency. Data leaks can expose sensitive information about

¹² Josh Fruhlinger (2018). The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet. CSO, March 9. <https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html>.

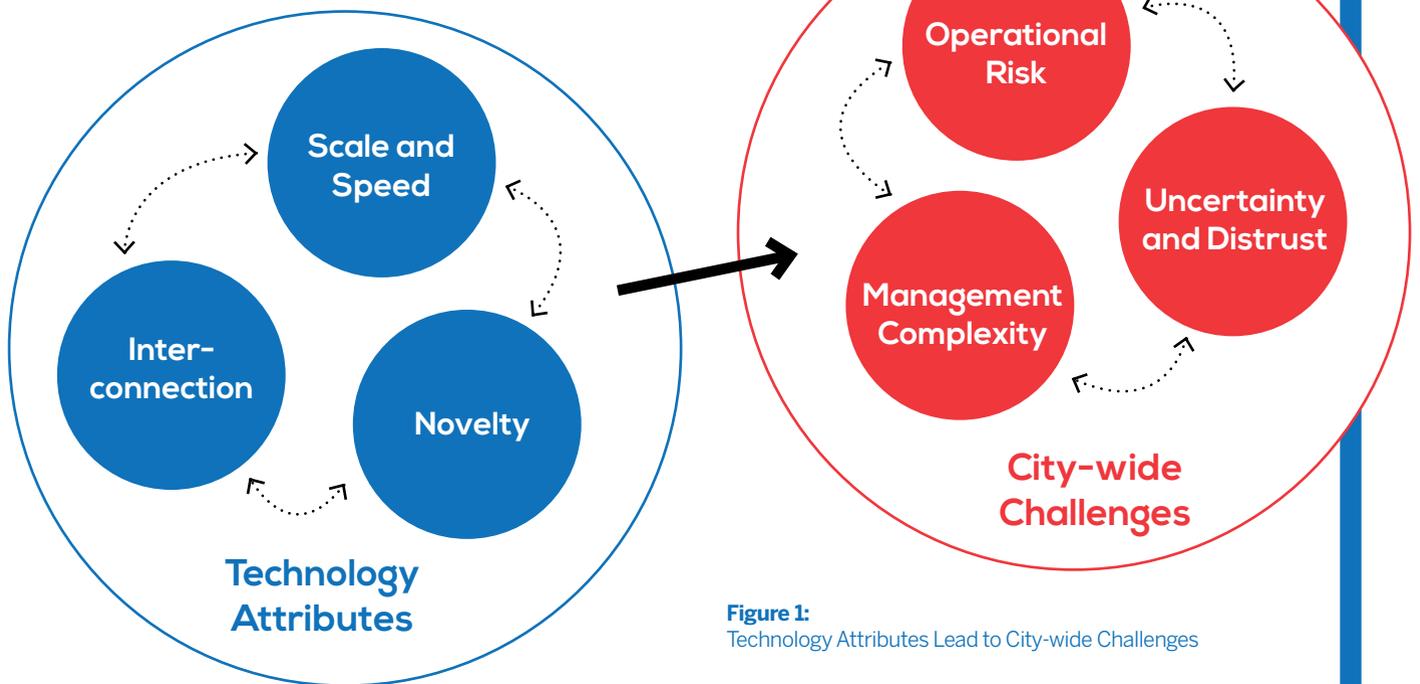


Figure 1:
Technology Attributes Lead to City-wide Challenges

citizens. Hacking and manipulation of industrial control systems can result in physical destruction and loss of life. Simply, the exponential proliferation of networked computing devices in the form of sensors coupled with limited city experience in deploying and appropriately configuring these devices substantially adds to a city's cyber risk. Smart Cities illustrate the conundrum that complexity can be an enemy of security.

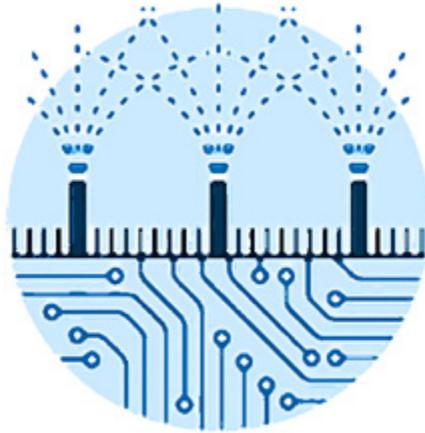
Thus, a principal source of heightened risk in the Smart City comes from increased reliance on technology. We have identified three **Technology Attributes** that are essential to the creation of Smart Cities, but also increase risk:

- **Scale and Speed:** the enormous number of smart devices rapidly deployed by multiple players;
- **Interconnection:** the unstructured networks that connect these devices are networked to each other and to critical infrastructure as well, creating complex interdependencies across services; and
- **Novelty:** the adoption of radically innovative technologies and capabilities.

These technology attributes combine to create three **City-wide Challenges**:

- Expanded **Operational Risk**;
- Increased **Management Complexity**; and
- New Levels of **Uncertainty and Distrust**.

This dynamic is illustrated in Figure 1.



Challenge #1: Expanded Operational Risk in the Smart City

Smart City executives operate in an environment of expanded technology-generated operational risk because of scale, interconnection and novelty. Each new device brings new opportunities and potential vulnerabilities. At scale, these devices and vulnerabilities are distributed across the city, often configured or deployed in ways unknown to most physical and cybersecurity managers.

Operated in silos, smart technology deployment often is divided along a city's operational domains. Budgeting and procurement processes reinforce these silos and hamper the integration of systems across critically important services, such as the integration of emergency communications and response across systems that support transportation and public safety. Organizational silos not only curtail the benefits of smart technology but may also expand operational risk when systems are interconnected without consideration for unanticipated dependencies and other security risks. The interconnection of these devices creates the danger of cascading failures due to complex—often unforeseen—technical and functional dependencies,

increasing consequences for the city and its inhabitants as they increasingly depend on cyber. Smart City executives must empower managers with responsibilities for technology and security, such as the Chief Technology and the Chief Information Security Officers, to manage the overall risk across a diverse technology and application landscape.

The novelty of Smart City technology creates steep learning curves for technology managers and users, increasing the risk of incorrect configuration, hacking and unintended interactions among systems. The shortage of skilled Smart City and cybersecurity personnel capable of managing new technologies exacerbates operational risk.¹³ Acquiring and retaining a talented ICT workforce in an already tight labor market is an uphill battle as local governments are competing against highly competitive salaries in the private sector.

The use of AI technologies to assist data handling and decisions introduces a major new risk dimension and increases the potential of unexpected and unpredictable outcomes that have neither obvious causes nor clear accountability. Finally, malicious actors, including trusted insiders, may exploit the new vulnerabilities to target smart infrastructure in cyber attacks and cause damage, steal information for financial gain, disrupt critical services, or attempt to influence decision-making and political processes.¹⁴ As city operations

¹³ A study finds that 40 percent of government officials see the lack of technical expertise as a primary challenge to launching Smart City projects. See: S. Bone (2018). Smart Cities Need a Smart Workforce. CompTIA. <https://www.aitp.org/blog/aitp-blog/2018/01/03/smart-cities-need-a-smart-workforce/>.

¹⁴ For a summary on recent cyber attacks on Smart Cities, see: Todd Thibodeaux (2017). Smart Cities Are Going to Be a Security Nightmare. Harvard Business Review, April 28. <https://hbr.org/2017/04/smart-cities-are-going-to-be-a-security-nightmare>.

become more dependent on technology, they become a more valuable target, as the 2018 ransomware on the City of Atlanta illustrated, which resulted in cost of up to 17 million USD for emergency response, system recovery and replacement.¹⁵



Challenge #2: Increased Management Complexity

Deployment of smart technologies also increases management complexity. Scale brings with it many ICT vendors offering a greater variety of products and services for use across multiple operational domains within a city. Smart Cities are being built upon existing infrastructure, not from scratch. As such, Smart Cities must manage multiple generations of technology, including administrative processes based on paper.

Interconnection increases management complexity by creating multiple

¹⁵ Ly Hay Newman (2018). Atlanta spent \$2.6m to recover from a \$52,000 Ransomware scare. Wired, April 23, 2018. <https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/>; Mathew Schwartz (2018). Atlanta's Reported Ransomware Bill: Up to \$17 Million. August 6. <https://www.bankinfosecurity.com/atlantas-reported-ransomware-bill-up-to-17-million-a-11281>.

pathways for corrupt data, or malware, to propagate hidden pockets of weak security and low resilience. The interdependencies created through interconnection make it difficult to isolate failure and clearly attribute risk and responsibility. Ownership of risk and liability is also hard to identify and assign; without clear assignment of responsibility for risk management, mitigation measures may go unimplemented.

Moreover, novelty can drive impulsive buying without due consideration of what it takes to derive value from investments in smart technologies. Enticed by seemingly compelling business cases, city officials often lack the capacity and resources to cut through the complexity of technology, processes, people and policies to capture anticipated benefits fully and mitigate new cybersecurity risks. Frameworks, standards and best practice guidance to steer functional integration and manage system complexity are still underdeveloped.¹⁶

Finally, complexity also applies to interactions with external stakeholders. Many aspects of what makes a city smart are not under the purview of local government officials. The boundaries between what city officials provide and what services private entities offer are fluid. The limited authority and capability of Smart City executives to coordinate services across the private sector adds to management complexity.

¹⁶ Note that global efforts towards establishing Smart City and IoT frameworks and standards, led by industry, academia and the public sector, have begun. Examples include NIST's Smart City Framework (International Technical Working Group on IoT-Enabled Smart City Framework), <https://pages.nist.gov/smartcitiesarchitecture/>; the IEEE Standards Associations' IoT related standards, <http://standards.ieee.org/innovate/iot/stds.html>; NTIA's Catalog of Existing IoT Security Standards (Version 0.01), https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog_draft_09.12.17.pdf.



Challenge #3: New Levels of Uncertainty and Distrust

The third challenge created by technology is heightened uncertainty and distrust. Unexpected behavior (“glitches”) in critical transportation or utility systems can undermine public confidence. Sensors enable detailed tracking of human activities across city infrastructure. While public engagement in emergencies and crime investigations has been cited as a breakthrough in improving a government’s ability to respond to emergencies and solve crimes,¹⁷ giving government such extensive information about private activities can also undermine trust.

More specifically, the sheer number of connected devices reduces managers’ awareness of what and who is on the network and what they are doing. Interconnection increases the challenge of modelling system behavior, opening uncertainty about how the systems will behave and interact, especially when stressed. Finally, technical novelty brings with it unknown immediate and longer-term vulnerabilities.¹⁸ More broadly, novelty hampers familiarity with what the new technology will do and why it does it. The latter is particularly relevant for machine learning and AI-based capabilities. Poorly understood disruptions in the established order and routine will not help build trust and acceptance.

¹⁷ Jeremy Armstrong (2018). New UK-wide evidence system set to ‘revolutionise crime fighting’. Belfast Live, April 16. <https://www.belfastlive.co.uk/news/new-uk-wide-evidence-system-14534706>.

¹⁸ See, for example, the discussion of the potential “hazardization” of IoT devices in Craig D. Spiegle (2018). Submission in response to NIST Request for Comments - NISTIR 8200. April 14. https://www.nist.gov/sites/default/files/documents/2018/04/16/ageight-nistir_8200-04142018.pdf.



Kibera, a marginalized community in **Nairobi**, was a “blank spot on the map” until young Kiberians created Map Kibera – a free and open community map that provides community information on security, water sanitation, health, and education. (mapkibera.org)



4 Responding to the City-wide Challenges

Responding to these challenges requires continual attention and strategic thinking—about people, processes and technology, as well as law and policy. As a shared responsibility, all stakeholders need to be involved.

The three city-wide challenges are closely interrelated: uncertainty and distrust exacerbate operational risk and management complexity; while unmanaged operational risk and insufficient management attention fuel uncertainty and distrust. All three challenges must be addressed in concert. Success is not a static end state. Responding to these challenges requires continual attention and strategic thinking—about people, processes and technology, as well as law and policy. As a shared responsibility, all stakeholders need to be involved.

Smart City executives should address the city-wide challenges by implementing a risk management framework, defining acceptable risk objectives and creating and testing an incident and emergency response plan. Risk management begins with a risk assessment, including assessment of uncertainties. Risks can then be reduced, transferred (e.g., via insurance) or simply borne to arrive at acceptable levels. In all cases, balancing the benefits of enhanced efficiency and effectiveness against the potential downsides is an essential part of risk management. Benefits must be managed actively to ensure that the anticipated value from technology deployment is realized. Smart City executives must clearly define benefits, determine control measures and weigh the cost of risk mitigation against the expected benefits.

For each of the four domains of action identified in the next section—cybersecurity, cyber resilience, privacy and data protection, and collaboration and coordination in governance—this Guide provides context and recommends actions Smart City executives should take. These measures aim at increasing stakeholders' trust that the Smart City is secure and resilient. Trustworthiness is a key driver in the acceptance and adoption of the Smart City concept by residents and businesses.

This section does not purport to present a comprehensive solution set. However, the actions we recommend, when taken together, will reduce substantially the downside risks created by these technology-induced, city-wide challenges.

Sound Cybersecurity Practice: Six Questions Smart City Executives Should Ask

1. How do we manage security governance across the city and with other governments, industry and the public?
2. What cybersecurity frameworks are we using, and why?
3. How are we mitigating our top five cybersecurity-related risks?
4. How prepared are the city's employees, enterprises and residents to execute their cybersecurity responsibilities?
5. How are external and internal threats evaluated and addressed?
6. What have we learned from exercising our cyber incident response plan?

Source: Questions inspired by ISACA, "Cybersecurity: What The Board of Directors Needs To Ask."
http://www.isaca.org/Knowledge-Center/Research/Documents/Cybersecurity-What-the-Board-of-Directors-Needs-to-Ask_res_Eng_0814.pdf?regnum=448554.



4.1 Cybersecurity: Connect Smart

Context

Sound cybersecurity practices are critical to ensuring the confidentiality, integrity and availability of Smart City services and data. Many cities have cybersecurity programs and have designated a responsible official to oversee implementation. Yet, maturity in these efforts vary widely. Officials should understand the traditional factors that contribute to enterprise cybersecurity risk (i.e., “risk” = “threats” x “vulnerabilities” x “consequences”—see Figure 2).¹⁹ They must work to achieve a security baseline reflecting the city’s chosen cybersecurity maturity level.²⁰

City executives can get a sense of the current state of their city’s overall cybersecurity by asking six key questions (see box on page 25). There are also many guides available to help technical staff reduce risk.^{21, 22}

This part of the Guide focuses on actions to manage the new risks to the safe and secure operation of cities that come with connecting innovative, Internet-enabled devices into established operational infrastructures, such as transportation systems and utilities, on a large scale.

Connecting Smart

Securing the Smart City, from complex industrial control systems to low-cost distributed sensors, requires an integrated approach that prevents, detects and mitigates the effects of attacks at every potentially vulnerable layer including devices, networks, applications and cloud platforms. Cybersecurity assets and programs must be positioned to prevent security incidents on a risk-informed basis, detect incidents when they occur and mitigate their impact. Importantly, cybersecurity does not stop at the city’s boundary; the city must share threat information and solutions with other cities, regional entities and expert communities to increase resilience and improve overall security capability.

¹⁹ An equally valid definition measures risk as the likelihood of an incident weighted by its impacts, so that an unlikely incident will present a high risk if its impact is large.

²⁰ ENISA (2017). Baseline Security Recommendations for IoT. November 20. <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>; and ENISA (2016). Architecture model of the transport sector in Smart Cities. January 12. <https://www.enisa.europa.eu/publications/smart-cities-architecture-model>. See also the maturity levels specified in the U.S. NIST Cybersecurity Framework, <https://www.nist.gov/cyberframework>.

²¹ Frameworks and standards to manage security and privacy risk in Smart Cities include the NIST Cybersecurity Framework (<https://www.nist.gov/cyberframework>), the ENISA Baseline Security Recommendations for IoT (<https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>), the Internet Society’s OTA IoT Trust Framework (<https://www.internetsociety.org/iot/trust-framework/>) and the Ethics & Algorithms Toolkit to manage algorithmic bias risk (<http://ethicstoolkit.ai/>).

²² For example, the Cyber Security Agency of Singapore (<https://www.csa.gov.sg/news/publications/be-safe-online>) recommends six essential cybersecurity measures: know your assets; allow only authorized software to work; timely patching and updating; give the right admin ‘passes’; detect breaches promptly; and strong access controls. Other useful cybersecurity resources include the Cybersecurity Campaign Playbook (<https://www.belfercenter.org/cyberplaybook>) and the CIS Controls (<https://www.cisecurity.org/controls/>).

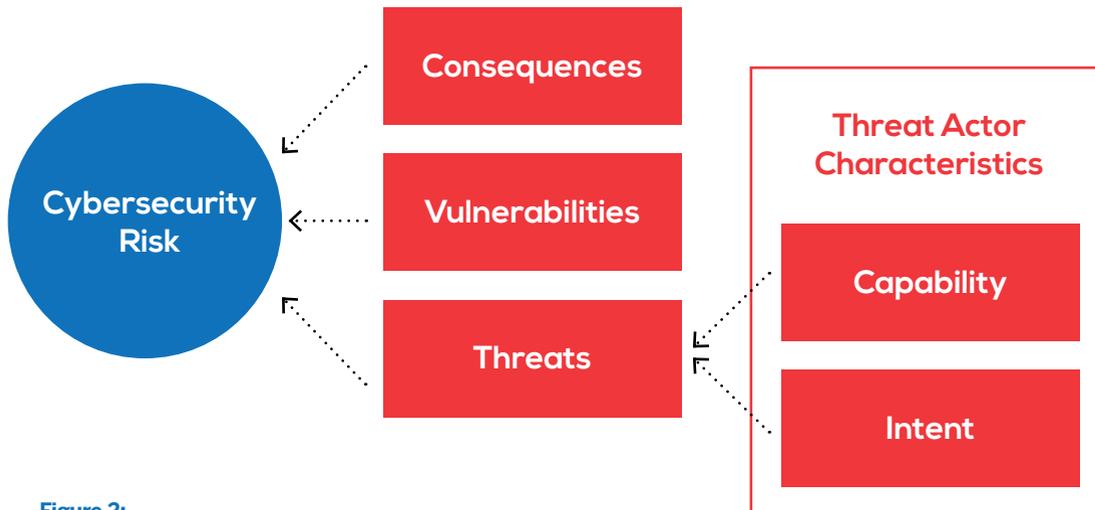


Figure 2:
Factors Contributing to Cybersecurity Risk

We have developed a general philosophy—“Connect Smart”—as a way to reduce cybersecurity risk and maximize benefits.²³ “Connect Smart” involves deciding when and how to connect devices and systems to each other. The approach comprises four elements:

1. Buy Secure: Know and enforce the following four key characteristics of secure devices through risk-informed procurement policies:²⁴

- Devices must be capable of accepting regular **patches and upgrades** to remove security vulnerabilities, ideally leveraging cryptographic integrity and authenticity protections.²⁵
- **Default passwords must be changeable** to user-defined and -managed passwords; two-factor authentication should be required. Products should support hardware-based authentication.
- **Device communications should be encrypted** with other devices and systems using cryptographic functions (lightweight encryption is now available even for small devices).

²³ Various leaders in cybersecurity have released or are working towards guidelines and recommendations regarding Smart City and IoT security, including ENISA (2017). Baseline Security Recommendations for IoT. <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>; Cyber Security Agency of Singapore (CSA) (2018). Be Safe Online Handbook. <https://www.csa.gov.sg/gosafeonline/resources/be-safe-online-handbook>; and the U.S. National Institute of Standards and Technology (NIST) (2018). Pre-Read Document for the NIST Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks Workshop. <https://www.nist.gov/sites/default/files/documents/2018/06/28/draft-iot-workshop-pre-read-document.pdf>.

²⁴ The EWI ICT Buyers Guide provides guidance on how to buy secure ICT products and services, based on risk-informed requirements and international standards. See: EWI (2016). Purchasing Secure ICT Products and Services: A Buyers Guide https://www.eastwest.ngo/sites/default/files/EWI_BuyersGuide.pdf.

²⁵ See also: Communicating Upgradability and Improving Transparency Working Group (2017). Communicating IoT Device Security Update Capability to Improve Transparency for Consumers. NTIA Multistakeholder Process on Internet of Things Security Upgradability and Patching. https://www.ntia.doc.gov/files/ntia/publications/communicating_iot_security_update_capability_for_consumers_-_jul_2017.pdf.



New York City's open data portal offers traffic data, urban planning metrics, city records, civic participation tools and various open data streams. (opendata.cityofnewyork.us)





Inti St Clair / Getty Images

- **Devices should be certified** (e.g., security labels), exhibit sound sourcing and development **provenance** and pass **conformance tests** based on recognized security certifications²⁶ and performed by independent third parties and published by the appropriate authority for verification.²⁷

2. Map and Manage the Networks: Use the network to enforce security.

- Create and maintain an **accurate inventory** of networked devices, applications and personnel, including their locations and status.
- **Segment and isolate networks** to control access and contain the spread of malware.
- **Report incidents** and anomalous traffic to a security information and event management system (SIEM).
- **Whitelist** legitimate applications and **blacklist** other applications.

3. Practice “Need to Know”: Exercise prudence when deciding to interconnect and run devices and applications. Legitimate data goes only where and when it is intended.

4. Authenticate Access: Every device should be authenticated. Internet-connected devices and infrastructure should take advantage of cloud-enabled authentication functions for IoT devices and for those who maintain them.²⁸ Move towards hardware-based strong authentication; do not rely on passwords alone.²⁹

²⁶ For example, Common Criteria for Information Technology Security Evaluation (<https://www.commoncriteriaportal.org>) and Common Criteria and the Federal Information Processing Standard 140-2 (FIPS 140-2) (<https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Standards>).

²⁷ Jan-Peter Kleinhans (2018). Standardisierung und Zertifizierung zur Stärkung der internationalen IT-Sicherheit. April. Stiftung Neue Verantwortung, Berlin. https://www.stiftung-nv.de/sites/default/files/standardisierung_und_zertifizierung.pdf.

²⁸ E.g., Amazon Web Services Developer Guide, at <https://docs.aws.amazon.com/iot/latest/developerguide/iot-security-identity.html>.

²⁹ FIDO Alliance (2017). The Future of Authentication for the Internet of Things. March 28. https://fidoalliance.org/wp-content/uploads/The_Future_of_Authentication_for_IoT_Webinar_170328_v10.pdf.

4.2 Cyber Resilience: Fail Safe

Context

Smart Cities face the risk of a major technology-related incident that could seriously degrade or disrupt city operations. Cyber resilience describes the ability of a city's complex cyber systems to continuously deliver critical outcomes despite everyday glitches and acute shocks.³⁰ Cyber resilience does not mean that no operation or infrastructure will fail, nor that a city is invulnerable to cyber attacks, but that it can adapt and recover.

Cyber resilience is a crucial part of urban resilience.³¹ Urban resilience depends on the smooth functioning of information technologies to perform and safeguard essential functions and to guarantee the safety and security of the public. To that end, cities rely on smart technologies to monitor daily operations and “vital signs” (e.g., pollution, traffic flows, seismic events), to coordinate emergency response activities (e.g., dispatch ambulances) and more generally to predict and respond to public safety incidents and emergencies. As with cybersecurity, resilience prioritization requires risk management.³²

A cyber incident can have wide-ranging effects. Cyber resilience must be coordinated across regions and nations, including network and cloud computing infrastructures operated by third parties. The City of Rotterdam in the Netherlands serves as a best practice exemplar. Its comprehensive 2016 resilience strategy addresses cyber resilience with measures to prepare the city's port and those who depend on it to mitigate potential ripple effects.³³

Failing Safe

Cyber resilience is about understanding and empowering the different layers that make up the operating fabric of the modern city—infrastructure, city operations and services, businesses, civil society and other organizations, as well as residents—so that they can “fail safe.”

“Failing safe” means expecting failure to occur and preparing for the potential consequences. Resilience requires creating alternatives that enable a flexible response.

³⁰ Adapted from: Cyber Resilience: Digitally Empowering Cities. <https://www.microsoft.com/en-us/cybersecurity/content-hub/cyber-resilience-digitally-empowering-cities>.

³¹ Resilience is a broad concept in the urban context. For an overview of “urban resilience,” see “What Is Urban Resilience?” at <http://www.100resilientcities.org/resilience>. IoT sensors and actuators can contribute to the overall resilience of a city by enabling early warning of environmental danger. The Guide focuses on keeping those and other critical capabilities functioning in the face of a technology-related incident.

³² NIST's “Standards for Security Categorization of Federal Information and Information Systems” introduces the concept of prioritizing assets for resilience measures. This allows city managers to assess and improve their security posture, given limited resources and increased system complexity due to IoT deployments.

³³ Rotterdam Resilience Strategy (2016). <https://www.100resilientcities.org/rotterdams-resilience-strategy/>.

“Failing safe” means that essential services remain available—even at reduced capacity, despite component or system failures—and will eventually bounce back. While individual organizations can improve their own cyber resilience, they are also dependent on other entities in the private and public sector.

There are many ways to increase resilience.³⁴ Under “Fail Safe,” we recommend three high-level courses of action:

1. Ensure Redundancy: Identify components central to Smart City operations where non-availability would have immediate and significant consequences, and ensure that they are designed with redundancy in mind.

- **Redundant infrastructure** for critical backbone networks is essential for Smart City operations. Building surplus capacity for resilience, however, is costly.
- **Alternative approaches** can also help maintain the availability of critical services. These include planned downgrades in the level of some services to keep the overall infrastructure running, temporary deployment of emergency procedures, and workarounds such as alternative, complementary technologies (e.g., mobile instead of wireline communications, dedicated emergency response networks, and fallback to physical controls or manual processes).
- A **critical data backup and recovery plan** should include storing data off-site and in multiple locations.³⁵ As with other technology management issues, redundancy usually has a technical as well as an organizational component—both need to be addressed to ensure resilience.

2. Design in Safety Defaults: Systems, devices and networks should be configured with failures in mind. If a system fails, a fallback system that is mirroring the main system can automatically replace it, or it can reboot or restart in a safe configuration, enabling the continuation of basic services until the situation that triggered the “fail safe” operation is corrected.

3. Test-Exercise-Adjust: To ensure that a system is resilient and prepared for business continuity, the systems, business processes and operators must be tested.³⁶ Testing includes stress-testing devices and infrastructures and simulating outages and incidents to evaluate responses. Exercising includes playing through response and recovery plans for various failure scenarios with the involvement of key stakeholders, along with unannounced exercises to gauge overall system and organizational resilience. Adjusting means periodically updating response plans and technology based on the lessons learned both from simulated and real incidents. The Test-Exercise-Adjust cycle must be a regular feature of Smart City operations.

³⁴ See, for example, the following frameworks: (1) WEF’s Partnering for Cyber Resilience (Maturity Model for Organizational Cyber Resilience), http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf; and (2) Microsoft’s Cyber Resilience: Digitally Empowering Cities, <https://www.microsoft.com/en-us/cybersecurity/content-hub/cyber-resilience-digitally-empowering-cities>.

³⁵ This can also help recover from ransomware attack.

³⁶ A series of ISO Standards provide guidance regarding the implementation of Business Continuity Management Systems: ISO 22317 - Guidelines for business impact analysis (BIA); (<https://www.iso.org/obp/ui/#iso:std:iso:ts:22317:ed-1:v1:en>); ISO 22313 – Guidance (<https://www.iso.org/obp/ui/#iso:std:iso:22313:ed-1:v1:en>); and ISO 22301 – Requirements (<https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-1:v2:en:sec:8.2.2>).

4.3 Privacy and Data Protection: Manage Responsibly

Context

In Smart Cities, cameras, microphones and other sensors collect abundant and comprehensive data about residents' physical, physiological, mental, economic, cultural, locational, communicative and social states. These technologies, together with open data initiatives, promise to increase the efficiency of services, foster economic prosperity and improve quality of life—including the safety and security of the public.³⁷ Yet, there is legitimate public concern about the privacy implications of the data collected and its use.

A recent survey by Unisys Corporation showed that citizens favored sensors (e.g., pacemakers, blood sugar monitors and smart phone alert buttons) that can alert medical professionals when one is in danger. Conversely, they were wholly unsupportive of the idea that law enforcement could use such devices to determine a person's location at their discretion.³⁸ Residents want to know that their data is collected ethically and in a transparent manner, retained and used for a specific purpose, and secured against unintended or unauthorized use. Thus, strong privacy and data protection is essential.³⁹ Absent such protections, Smart City executives will encounter tremendous barriers to establish the trust necessary for successful adoption.⁴⁰

Privacy should not be an afterthought in Smart City development. Smart City executives must raise awareness and engage community groups to determine appropriate measures towards acceptable privacy solutions. Technology vendors, software and device manufacturers, as well as policymakers and regulators must recognize the inextricable relationship between privacy and security from the outset and find sound technical and regulatory solutions to the new privacy challenges Smart Cities create. As with technology professionals, privacy professionals are in short supply—but essential to public trust.

Around the world, consumers are increasingly pushing for increased transparency, clarity and notification of practices affecting their privacy and individual information rights. Effective as of May 2018, the General Data Protection Regulation (GDPR) strengthens the protection of personal data in the European Union (EU) and for EU citizens globally. China's 2017 Cybersecurity Law introduced measures and implemented fines for data protection violations. In the United States, the Supreme Court has ruled that a fundamental right to privacy is guaranteed in the Constitution,

37 A. Bartoli (2012). "On the Ineffectiveness of Today's Privacy Regulations for Secure Smart City Networks," in Proceedings of Third IEEE International Conference on Smart Grid Communications.

38 A 2017 survey conducted in 13 countries across North America, Latin America, Europe, and Asia Pacific. Unisys Security Index, Unisys Report on the global results of the 2017 Unisys Security Index, <http://www.unisys.com/unisys-security-index>.

39 The report uses the notions of data protection and privacy interchangeably, referring to the measures employed to ensure that sensitive, personal information (personally identifiable information or PII) is handled in accordance to widely agreed privacy principles. In the U.S. and India "privacy" is commonly used, whereas "data protection" is more prevalent in the European Union and China.

40 A 2016 study by the U.S. National Telecommunications and Information Administration (NTIA) found that lack of trust in Internet privacy and security may deter online activities. See <https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>.

a notion that has evolved as information technology has expanded.⁴¹ Similarly, India's Supreme Court ruled in 2017 that privacy is a fundamental, constitutional right. The Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules were developed in collaboration with industry and civil society "to build consumer, business and regulator trust in cross border flows of personal information" and endorsed by heads of state in 2011.⁴²

Widely-Agreed Privacy Principles:⁴³

To ensure privacy and protect data, entities providing services in the Smart City and processing sensitive data must adhere to certain guiding principles—and to national laws—governing data protection and privacy. The principles guide the collection, processing, retention and maintenance of data in a secure and fair manner.

- 1. Preventing harm:** Privacy protections should prevent harmful collection or misuse of personal information and remedies for infringement should be proportionate to the severity of harm.
- 2. Notice:** Data controllers should notify individuals when collecting personal information before or at the time of data collection, or as soon after as is reasonably practical.
- 3. Collection limitation:** Personal information should be collected with, where appropriate, the consent of or notice to the data subject, and be limited to information relevant to the collector's purpose.
- 4. Uses of personal information:** Data collectors should only use personal information to fulfill the purpose of collection or other compatible purposes.
- 5. Choice:** Individuals should be provided with mechanisms to exercise choice in how their personal information is collected, retained, used and disclosed.
- 6. Integrity of personal information:** Personal information should be kept accurate, complete and current to the extent necessary for the purpose of use.
- 7. Security safeguards:** Data controllers are responsible for securing personal information to the degree appropriate to its sensitivity, context and the likelihood of harm.
- 8. Access and correction:** Individuals have a right to access and correct their personal information.
- 9. Accountability:** Data controllers are accountable for complying with the above principles and should also take steps to ensure that recipients of any transferred information protect the data in a consistent manner.



41 See for example, *Carpenter v. United States*, 585 U.S. __ (2018). The U.S. Federal Trade Commission (FTC) urged businesses and manufactures to adopt best practices to protect users' privacy (FTC (2015). *Internet of Things: Privacy & Security in a Connected World*. FTC staff report, January. <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>) and has taken enforcement action against companies whose IoT products put users' privacy at risk.

42 "Cross Border Privacy Rules System." See <http://www.cbprs.org>.

43 Based on the principles outlined in the 2005 Privacy Framework endorsed by APEC leaders, see <https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework>; and <https://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-data-protection>.



Rio de Janeiro's crime mapping system, ISP GEO, digitizes, standardizes, and disseminates geospatial and temporal data. It complements the CrimeRadar mobile app, which makes crime levels transparent to the public and helps people navigate the city. (igarape.org.br)



Managing Responsibly

Smart Cities face some unique privacy and data protection challenges. They need to be addressed by technical and organizational measures to ensure public trust and acceptance regarding the collection, retention, processing and analysis of data. Sound data security practice is a necessary, but insufficient, condition to ensure privacy and data protection. Cities should, at a minimum, follow the basic privacy and data protection principles agreed to in many countries (see box on page 33 with principles based on the APEC Privacy Framework) and seek cooperation with the respective regulatory and data protection authorities. To help implement these principles, we recommend three specific actions particularly applicable to Smart Cities for the privacy and data protection of residents and enterprises:

1. Proclaim a Privacy and Data Protection Charter: Develop and publish a Privacy and Data Protection Charter that enshrines privacy-by-design and privacy-by-default approaches in the development and deployment of Smart City applications and applies strict privacy settings by default.⁴⁴ These approaches make privacy a proactive notion and build trust with residents and users. Smart City executives should champion privacy-preserving technologies and encourage (or mandate where possible) high standards regarding data protection, including through procurement policy. Technical and organizational guidelines complement the charter by prescribing best practices and standards to enhance privacy and implement data minimization, including (a) data retention, (b) data anonymization and pseudonymization, (c) privacy notices, (d) data sharing, (e) encryption of personally identifiable information and (f) notification requirements when breaches occur.⁴⁵ The charter should also acknowledge the principled tradeoffs that must be made between protecting privacy and providing data access to law enforcement.

2. Enhance Transparency and Appoint a Chief Privacy Officer: Regular public reporting on the state of privacy and data protection in the Smart City enables transparency and oversight by the public. For critical domains, a regular privacy impact assessment should be performed and the results released to the public. In larger cities, a designated chief privacy officer can act as an ombudsman who takes on a visible role in oversight, advocates for data protection and privacy and ensures compliance with privacy and data protection laws.

3. Require Data Governance Agreements with Third Parties: For sensitive information that is processed by third parties (including other public agencies or private parties), whether as service providers or as customers, a data governance agreement should spell out what information is covered, who owns it and under what conditions they may use it.⁴⁶ The agreement describes roles and accountability for data processing, clarifies who owns and is responsible for the data and ensures adherence to the Smart City's Privacy and Data Protection Charter.

⁴⁴ Privacy by Design Primer: <https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf>; What does data protection 'by design' and 'by default' mean?: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en.

⁴⁵ As an example, see how the City of New York addresses privacy issues in its Smart City efforts: NYC Guidelines for the Internet of Things, Privacy + Transparency. <https://iot.cityofnewyork.us/privacy-and-transparency>.

⁴⁶ Gwen Thomas, "Defining Data Governance," Data Governance Institute, <http://www.datagovernance.com/defining-data-governance/>.

4.4 Collaboration and Coordination in Governance: Govern Inclusively

Context

The technical complexity of securing smart environments with millions of devices, networks and cloud platforms is exceeded only by the organizational challenges it creates. Residents and businesses produce and consume Smart City services often in loose, ad hoc arrangements. In most cases, they pay little attention to security, assuming that it is being managed for them. Powerful companies may push Smart City developments in directions that do not consider the long-term interests of the city, its residents and business (e.g., by demanding unreasonable access to personal data). In the race to attract global investments and lead digital innovation, cities may prematurely buy untested technologies that inadvertently create new risk which is not well-understood at the time of deployment. Given the relatively immature stage of smart technologies, cities should be cautious in making concessionary long-term investments. Officials at the local, regional and national levels must monitor such developments and intervene firmly when and where necessary to balance public and private interests.

It is the task of Smart City executives to create a culture, and build structures, processes, mechanisms and incentives that efficiently enable effective collaboration and coordination, ensure coherence, and promote coalescence around shared values.⁴⁷ To achieve cybersecurity, resilience and privacy, it is important to engage experts and residents—the former for their knowledge, the latter to hear concerns, gather local knowledge and feedback, manage expectations, and ultimately build trust.

Collaboration and coordination in governance are complicated by two principal factors:

- **Fluid Boundaries and Limited Authorities:** The political and organizational boundaries of a Smart City are difficult to define and change over time, fed by the distributed nature of the technology infrastructure. Assigning and exercising responsibility for risk management are challenging tasks for Smart City executives.
- **Cultural Diversity and Disparate Visions:** Cities are not monolithic. Attitudes toward government, privacy and security differ across cultures. Multiple governmental, commercial and civil society stakeholders are engaged. Entities connecting their devices and providing services have different objectives, which may or may not align with a Smart City's overall vision. As characteristics of cities differ, so must the approaches to securing them.

⁴⁷ See also, ENISA (2017). Cyber Security Culture in organizations. November. <https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations>.

Governing Inclusively

Four principles lay the foundation for sound collaboration and coordination in governance:

- **Transparency:** The city's administration has an obligation to share information with its residents and businesses. Transparency is at the heart of the accountability and trust needed to ensure the city's cybersecurity and resilience.
- **Accountability:** Responsibility for achieving outcomes must be clear for both private and public entities, driving the implementation of proven security concepts and technology.
- **Participation:** Relevant stakeholders, public and private, must be engaged to effectively recognize threats to the Smart City and mitigate them. Inclusive collaboration and coordination take place on multiple levels—at the city and regional level and across the wider ecosystem. Residents' involvement, through town hall meetings and other means, is critical to achieve acceptance and adoption, and to ensure that initiatives consider the needs of all residents.
- **Leadership:** In the end, the municipality and its elected officials bear final responsibility for the secure and resilient development of Smart Cities. Weighing individual and private interests against the public interest, finding the balance and committing to its achievement are the core of leadership.

Based on these principles, to ensure effective collaboration and coordination and sound governance, we recommend three courses of action:

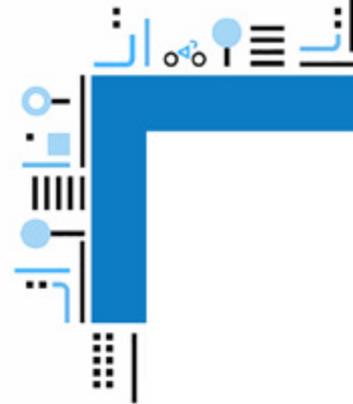
1. Deploy Collaboration and Coordination Platforms: Online forums and digital tools can facilitate the sharing of best practices, exchanging relevant data and sharing opinions and suggestions. Such platforms should be a central part of the Smart City strategy, as they can enable crowdsourced solutions from diverse groups of stakeholders.

2. Organize for Engagement: Smart City executives may showcase leadership by spearheading roundtables on specific topics and leading regional clusters to debate and resolve issues. Engagement with marginalized communities is particularly important to ensure that the deployment of smart technologies does not exacerbate existing inequalities.

3. Communicate Clearly and Often: Decisions ultimately reflect hard trade-offs regarding security, privacy and budget priorities. Clear messaging about decisions and their rationale will build trust and inclusivity.

5 Creating a Roadmap Towards a Secure and Resilient City

The implementation of security and resilience into a Smart City is complex and should be part of every Smart City planning effort.

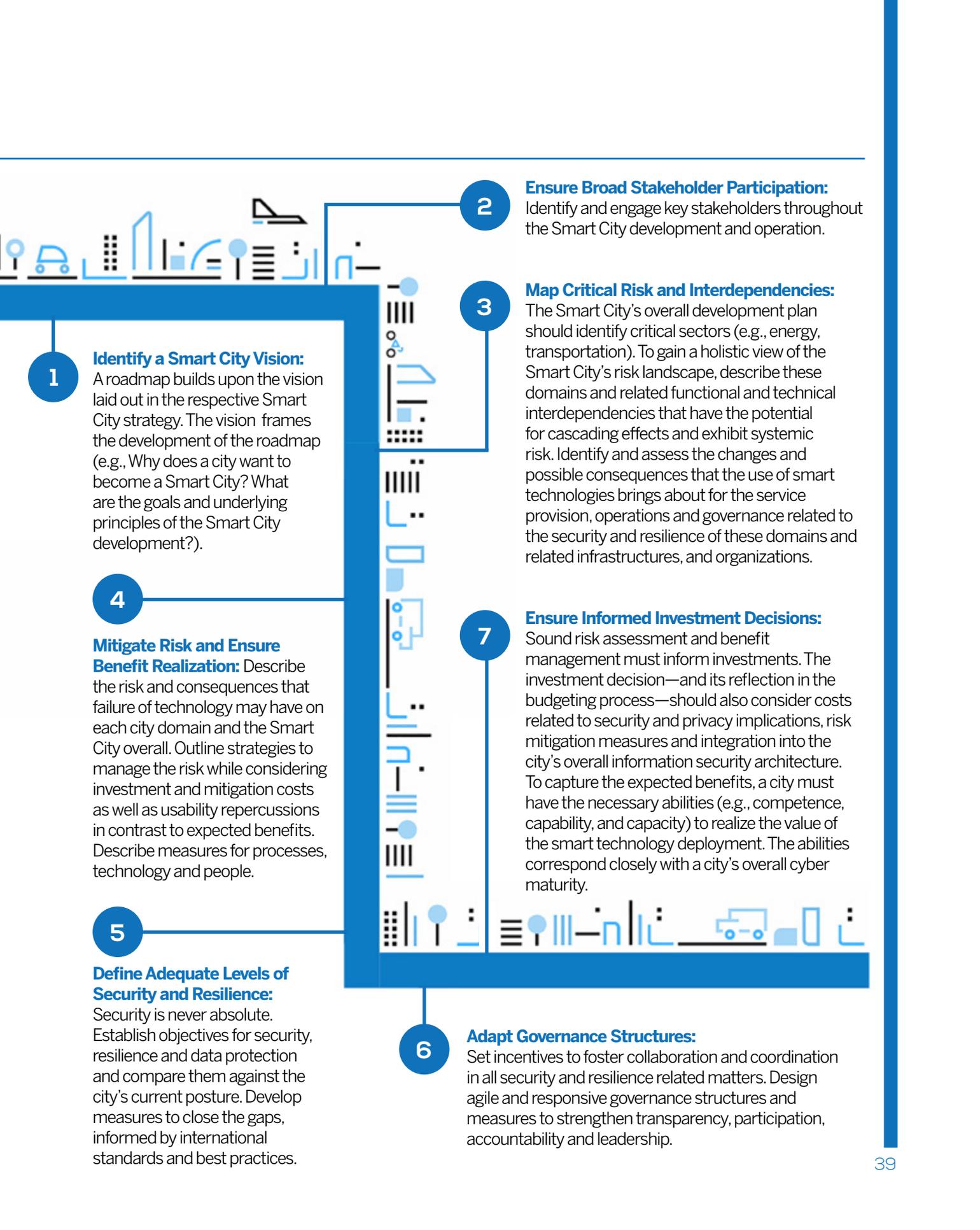


However, considerations of security and resilience are often an afterthought, mistakenly left to the IT department rather than spearheaded by the city's senior leadership. As such, we recommend that Smart City managers develop a roadmap. The recommendations outlined in this Guide—Connect Securely, Fail Safe, Manage Responsibly and Govern Inclusively—should support the roadmap development.

A roadmap has three functions. First, it serves as a guide post; it tells everyone where their city stands and helps them get to where they want to go. Second, it is a call to action for broad engagement of all stakeholders. Importantly, roadmap development allows for dialogue among stakeholders, creates a common vision, promotes understanding of the problems and their solutions, and helps identify the best path forward. Third, it considers internal and external aspects of the environment and how these factors will shape the development of the Smart City (e.g., growth of the city, changes to the legal and regulatory environment, and progress in technology).

A roadmap for security and resilience incorporates the vision and values from the overall Smart City initiative and determines goals, strategies and actions that ensure security, resilience and data protection on the ground, and establishes structures and processes for sound collaboration and coordination in governance. The roadmap further addresses potential roadblocks and determines milestones to track and communicate progress during the implementation.

Cities vary in size, organization, culture and style of governance. Independent of a city's overall structure, the key elements a roadmap should include:



1

Identify a Smart City Vision:

A roadmap builds upon the vision laid out in the respective Smart City strategy. The vision frames the development of the roadmap (e.g., Why does a city want to become a Smart City? What are the goals and underlying principles of the Smart City development?).

4

Mitigate Risk and Ensure Benefit Realization:

Describe the risk and consequences that failure of technology may have on each city domain and the Smart City overall. Outline strategies to manage the risk while considering investment and mitigation costs as well as usability repercussions in contrast to expected benefits. Describe measures for processes, technology and people.

5

Define Adequate Levels of Security and Resilience:

Security is never absolute. Establish objectives for security, resilience and data protection and compare them against the city's current posture. Develop measures to close the gaps, informed by international standards and best practices.

2

Ensure Broad Stakeholder Participation:

Identify and engage key stakeholders throughout the Smart City development and operation.

3

Map Critical Risk and Interdependencies:

The Smart City's overall development plan should identify critical sectors (e.g., energy, transportation). To gain a holistic view of the Smart City's risk landscape, describe these domains and related functional and technical interdependencies that have the potential for cascading effects and exhibit systemic risk. Identify and assess the changes and possible consequences that the use of smart technologies brings about for the service provision, operations and governance related to the security and resilience of these domains and related infrastructures, and organizations.

7

Ensure Informed Investment Decisions:

Sound risk assessment and benefit management must inform investments. The investment decision—and its reflection in the budgeting process—should also consider costs related to security and privacy implications, risk mitigation measures and integration into the city's overall information security architecture. To capture the expected benefits, a city must have the necessary abilities (e.g., competence, capability, and capacity) to realize the value of the smart technology deployment. The abilities correspond closely with a city's overall cyber maturity.

6

Adapt Governance Structures:

Set incentives to foster collaboration and coordination in all security and resilience related matters. Design agile and responsive governance structures and measures to strengthen transparency, participation, accountability and leadership.

6 Conclusion

Only by staying ahead of the curve will executives fully realize benefits, prevent technical failures and defend against cyber crime.

The gains and risks from deploying smart technologies to develop a Smart City are real and significant. All involved in Smart City efforts must keep in mind that the ultimate goals—which may vary from city to city—are improved outcomes that serve the people including but not limited to equity, safety, health, growth, inclusiveness and sustainability. Managing these smart technologies, including measures to ensure cybersecurity, resilience and privacy, but also the structures, mechanisms and incentives to govern the technologies and their security is only a means to an end, and should not be mistaken as an end in itself.

Smart Cities run on new technologies, novel systems and complex networks designed to supervise and deliver services to the public, local businesses and government. Such environments that interconnect the physical and the digital are likely to exhibit unexpected behavior and new risk. Cities invest in these new technologies, expecting a return. Yet, the risk of these technologies must be managed and benefits must be tracked to ensure their realization. Both present a significant challenge, because they manifest in different venues,

including technology itself, but also process, policy, law and, in particular, people. Smart Cities require constant learning and innovation. Only by staying ahead of the curve will executives fully realize benefits, prevent technical failures and defend against cyber crime.

Cities are different—so will be the choices of small cities, regional capitals or megacities. The maturity to deploy technology and capably manage risk and benefits will play an important role. A city's size and density, history, culture, economic strength, and future outlook will shape this calculus, as will its embeddedness in the larger national or regional structures as well as policy and legal frameworks.

It is also important to recognize the limitations of the promises that technology holds for the future of the urban environment. When considering the deployment of these technologies, city managers and decision-makers should not forget the significant challenges cities have long been trying to overcome, including poverty and homelessness, systemic corruption, ecological breakdowns and infrastructure disrepair, among many other issues impacting quality of life.



Technology has a role to play in helping to solve these problems, but solutions need to go beyond technical innovation and smart deployment to also include social and institutional changes. The greatest challenge presented by Smart Cities—and the future of urban living—will be a human one. Ultimately, the responsibility of implementing Smart

Cities will rest with the city's leadership. Yet, practical experience in managing such large and complex systems is rare. Cooperation and collaboration across cities and nations will prove essential to the successful functioning of Smart Cities—and to public acceptance and trust in the Smart City vision.

7 Appendix – Defining Key Terms: Smart Technologies

Cloud Computing

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”⁴⁸

Internet of Things (IoT)

The Internet of Things (IoT) builds upon the infrastructure, services, and processes of the Internet and is defined as: “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.”⁴⁹

Networks

Networks enable devices (such as computers, sensors and other IoT devices) to communicate through physical or wireless electronic communications technologies and protocols. Current relevant network communications technologies and protocols for Smart Cities include 4G LTE (Long Term Evolution), GSM (Global System for Mobile communication), CDMA (Code Division Multiple Access), Wi-Fi, Bluetooth, NFC (Near-Field Communication), ZigBee (open wireless standard) and Z-Wave (wireless communication).⁵⁰ The next wave of mobile networks will deploy faster 5G technologies and protocols in the near future.

Artificial Intelligence (AI)

Artificial Intelligence (AI) enables computers and machines to perform “smart” tasks that would require human intelligence, including visual perception, decision-making, contextual understanding and emotion detection.

Machine Learning (ML)

Machine learning (ML) involves providing a computer system with algorithms and “real world” data, which enable the system to learn, improving its ability to understand the preferences of users and support decision-making in increasingly complex decisions and situations.

⁴⁸ SP 800-145, The NIST Definition of Cloud Computing <https://csrc.nist.gov/publications/detail/sp/800-145/final>.

⁴⁹ International Telecommunication Union (2012). ITU-T Y.2060, June. <https://www.itu.int/rec/T-REC-Y.2060-201206-I>.

⁵⁰ Rob Kitchin, Martin Dodge (2017). The (in)security of smart cities: vulnerabilities, risks, mitigation and prevention. The Programmable City Working Paper 24. February 13. <https://osf.io/preprints/socarxiv/f6z63>.

Acknowledgments

This report was prepared by the EastWest Institute and authored by **Andreas Kuehn** and **Bruce McConnell**. The authors are extremely grateful for the advice provided by the experts listed below. Their inclusion here does not mean that they support or agree with any of the report's statements, proposals, recommendations or conclusions. In particular, the report greatly benefited from the expertise and experience of the leaders of the EWI Breakthrough Group on Secure, Resilient Cities and the Internet of Things, who led working sessions and provided key inputs to the paper:

Benedikt Abendroth, Senior Cybersecurity Strategist, Microsoft
Mark Forman, Global Head, Public Sector, Unisys
Sami Nassar, Vice President, Cybersecurity Solutions, NXP Semiconductors
Jim Pinter, Senior Partner Strategy Manager, Microsoft
Andy Purdy, Chief Security Officer, Huawei Technologies USA

The following experts provided substantive commentary and advice during the development of this Guide:

Chuck Benson, Co-Chair, UW Compliance IoT Risk Mitigation Task Force, University of Washington
Jeffrey Brown, Manager, Future of Work and Artificial Intelligence, Bertelsmann Foundation
Aaron Clark-Ginsberg, Associate Social/Behavioral Scientist, RAND Corporation
Gwenda Fong, Director (Strategy), Cyber Security Agency of Singapore
Gaurav Garg, Director of Information Technology/CIO, City of Santa Clara
Udo Helmbrecht, Executive Director, European Union Agency for Network and Information Security (ENISA)
Ammar Jaffri, Chief Executive, E-Pakistan; Director General, Center of Information Technology, Pakistan
Jan-Peter Kleinhans, Project Director IoT Security, Stiftung Neue Verantwortung
Apostolos Malatras, Network and Information Security Expert, European Union Agency for Network and Information Security (ENISA)
Tim Polk, Director, International Standards, NIST
Tom Ray, Information Security Manager/CISO, City of Berkeley
John E. Savage, An Wang Professor Emeritus of Computer Science, Brown University
Stefan Schiffner, Postdoctoral Research Associate, SECAN-Lab, University of Luxembourg
Craig Spieziele, Managing Partner, AgeLight Advisory Group; Founder/Chairman Emeritus, Online Trust Alliance
Leonie Tanczer, Lecturer in International Security and Emerging Technologies, Department of Science, Technology, Engineering and Public Policy, University College London
Jason Whittet, Associate Director, 100 Resilient Cities

The following EWI associates provided invaluable support and assistance for this report:

Elizabeth Chen, Michael Depp, Conrad Jarzebowski, Abigail Lawson, Anneleen Roggeman, Alex Schulman, Spandana Singh and **Dragan Stojanovski**.

Board of Directors

OFFICE OF THE CHAIRMAN

Ross Perot, Jr. (U.S.)

Chairman
EastWest Institute
Chairman
Hillwood Development Co. LLC

R. William Ide III (U.S.)

Counsel and Secretary
Chair of the Executive Committee
EastWest Institute
Partner
Dentons US LLP

Amb. Cameron Munter (U.S.)

CEO and President
EastWest Institute
Former Ambassador
Embassy of the United States to Pakistan

CO-FOUNDERS

John Edwin Mroz† (U.S.)

Former President and CEO
EastWest Institute

Ira D. Wallach† (U.S.)

Former Chairman
Central National-Gottesman Inc.

MEMBERS

Peter A. Altabef (U.S.)

Chairman and CEO
Unisys Corporation

Hamid Ansari (U.S.)

President and Co-Founder
Prodea Systems, Inc.

Tewodros Ashenafi (Ethiopia)

Chairman and CEO
Southwest Energy (HK) Ltd.

Mark Joseph Bild (U.S.)

Managing Partner
BAI Corporation

Mary McInnis Boies (U.S.)

Counsel
Boies, Schiller & Flexner LLP

Sir Peter Bonfield (U.K.)

Chairman
NXP Semiconductors

Matt Bross (U.S.)

Chairman and CEO
Compass-EOS

Robert N. Campbell III (U.S.)

Founder and CEO
Campbell Global Services LLC

Maria Livanos Cattau (Switzerland)

Former Secretary-General
International Chamber of Commerce

Michael Chertoff (U.S.)

Executive Chairman and Co-Founder
The Chertoff Group
Former Secretary of the U.S. Department of Homeland Security

David Cohen (Israel)

Chairman
F&C REIT Property Management

Roger Cohen (U.S.)

Op-Ed Columnist
The New York Times

Joel H. Cowan (U.S.)

Professor
Georgia Institute of Technology

Addison Fischer (U.S.)

Chairman and Co-Founder
Planet Heritage Foundation

Stephen B. Heintz (U.S.)

President
Rockefeller Brothers Fund

Hon. Steven S. Honigman (U.S.)

Counselor
Information and Infrastructure Technologies, Inc.

Dr. Hu Yuandong (China)

Chief Representative
UNIDO ITPO-China

John Hurley (U.S.)

Managing Partner
Cavalry Asset Management

Amb. Wolfgang Ischinger (Germany)

Chairman
Munich Security Conference

Ralph Isham (U.S.)

Managing Director
GH Venture Partners LLC

Anurag Jain (U.S.)

Chairman
Access Healthcare

Gen. (ret) James L. Jones (U.S.)

Former U.S. National Security Advisor
Former Supreme Allied Commander Europe
Former Commandant of the Marine Corps

George Kadifa (U.S.)

Managing Director
Sumeru Equity Partners

Haifa al Kaylani (Lebanon/Jordan)

Founder and Chairperson
Arab International Women's Forum

Sezgin Baran Korkmaz (Turkey)

CEO
SBK Holding

Zuhal Kurt (Turkey)

Chairman of the Board
Kurt Group

Gen. (ret) T. Michael Moseley (U.S.)

President and CEO
Moseley and Associates, LLC
Former Chief of Staff
United States Air Force

Karen Linehan Mroz (U.S.)

President
Roscommon Group Associates

F. Francis Najafi (U.S.)

CEO
Pivotal Group

Amb. Tsuneo Nishida (Japan)

Professor
The Institute for Peace Science at Hiroshima University
Former Permanent Representative of Japan to the United Nations

Admiral (ret)**William A. Owens (U.S.)**

Chairman
Red Bison Advisory Group LLC

Dr. William J. Parker III (U.S.)

President and CEO
National Defense University Foundation

Sarah Perot (U.S.)

Director and Co-Chair for Development
Dallas Center for Performing Arts

Laurent M. Roux (U.S.)

Founder and President
Gallatin Wealth Management, LLC

Mike Sarimsakci (Turkey)

Founder and President
Altterra International, LLC

Ikram ul-Majeed Sehgal (Pakistan)

Chairman
Security & Management Services Ltd.

Amb. Kanwal Sibal (India)

Former Foreign Secretary of India

Kevin Taweel (U.S.)

CEO
Asurion

Alexander Voloshin (Russia)

Chairman of the Board
JSC Freight One (PGK)
Non-Executive Director
Yandex Company

Adm. Patrick M. Walsh (U.S.)

Vice President
U.S. Navy and Marine Corps Services
Boeing Global Services

Amb. Zhou Wenzhong (China)

Secretary-General
Boao Forum for Asia

NON-BOARD COMMITTEE MEMBERS**Hilton Smith, Jr. (U.S.)**

President and CEO
East Bay Co., LTD

CHAIRMEN EMERITI**Martti Ahtisaari (Finland)**

2008 Nobel Peace Prize Laureate
Former President of Finland

Berthold Beitz† (Germany)

President
Alfried Krupp von Bohlen und
Halbach-Stiftung

Ivan T. Berend (Hungary)

Professor
University of California, Los Angeles

Francis Finlay (U.K.)

Former Chairman
Clay Finlay LLC

Hans-Dietrich Genscher† (Germany)

Former Vice Chancellor and Minister of
Foreign Affairs of Germany

Donald M. Kendall (U.S.)

Former Chairman and CEO
PepsiCo Inc.

Whitney MacMillan (U.S.)

Former Chairman and CEO
Cargill Inc.

Mark Maletz (U.S.)

Former Chairman, Executive Committee
EastWest Institute
Senior Fellow
Harvard Business School

George F. Russell, Jr. (U.S.)

Chairman Emeritus
Russell Investment Group
Founder, Russell 20-20

H.E. Dr. Armen Sarkissian (Armenia)

President
Republic of Armenia

DIRECTORS EMERITI**Jan Krzysztof Bielecki (Poland)**

CEO
Bank Polska Kasa Opieki S.A.
Former Prime Minister of Poland

Emil Constantinescu (Romania)

President
Institute for Regional Cooperation and
Conflict Prevention (INCOR)
Former President of Romania

William D. Dearstyne (U.S.)

Former Company Group Chairman
Johnson & Johnson

John W. Kluge† (U.S.)

Former Chairman of the Board
Metromedia International Group

Amb. Maria-Pia Kothbauer (Liechtenstein)

Ambassador of Liechtenstein to Austria,
the OSCE and the United Nations in Vienna

William E. Murray† (U.S.)

Former Chairman
The Samuel Freeman Trust

John J. Roberts (U.S.)

Senior Advisor
American International Group (AIG)

Daniel Rose (U.S.)

Chairman
Rose Associates Inc.

Leo Schenker (U.S.)

Former Senior Executive Vice President
Central National-Gottesman Inc.

Mitchell I. Sonkin (U.S.)

Managing Director
MBIA Insurance Corporation

Thorvald Stoltenberg† (Norway)

President
Norwegian Red Cross

Liener Temerlin (U.S.)

Chairman
Temerlin Consulting

John C. Whitehead† (U.S.)

Former Co-Chairman
Goldman Sachs
Former U.S. Deputy Secretary of State

† Deceased

Copyright © 2018 EastWest Institute
Photos: Getty Images

The EastWest Institute works to reduce international conflict, addressing seemingly intractable problems that threaten world security and stability. We forge new connections and build trust among global leaders and influencers, help create practical new ideas, and take action through our network of global decision-makers. Independent and nonprofit since our founding in 1980, we have offices in New York, Brussels, Moscow and San Francisco.

EastWest Institute
10 Grand Central
155 E. 44th Street, Suite 1105
New York, NY 10017 U.S.A.
+1 (212) 824-4100

communications@eastwest.ngo
www.eastwest.ngo

City Data Exchange, an open data portal of **Copenhagen**, is enabling purchasing, selling and sharing a broad range of commercial data types between all kinds of users in a city – citizens, public institutions and private companies. (cphsolutionslab.dk)





Global Cooperation in Cyberspace

SUPPORTERS:

Microsoft
Huawei Technologies
Unisys
Qihoo 360
NXP Semiconductors
CenturyLink
JPMorgan Chase
Marsh & McLennan
The Hague Centre for Strategic Studies

PARTNERS:

William and Flora Hewlett Foundation
IEEE Communications Society
Global Forum on Cyber Expertise
Munich Security Conference
M³AAWG
The Open Group
Fudan University
University of New South Wales
Center for Long-Term Cybersecurity, University of California, Berkeley



New York | Brussels | Moscow | San Francisco
www.eastwest.ngo | [t: @EWInstitute](https://twitter.com/EWInstitute) | [f: EastWestInstitute](https://facebook.com/EastWestInstitute)