SECURITY TECHNOLOGY EXECUTIVE

RISK MITIGATION STRATEGIES AND SOLUTIONS • JULY/AUGUST 2019 • VOL. 29/NO. 3

POWERED BY SIW SECURITY INFOWATCH.COM

How to Secure a Smart City

Interoperability, Sense and Sensibility

Page 18

ENDEAVOR BUSINESS MEDIA

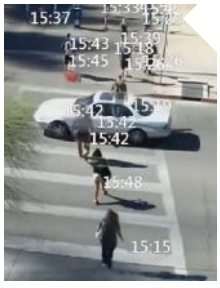
SECURITY TECHNOLOGY EXECUTIVE

18

COVER STORY

Interoperability, Sense and Sensibility: Foundation for a Small City

By Steve Surfaro



How to Secure Smart Cities in an Era of Change

Cities have yet to come to grips with the implications of their changing ecosystems, or for that matter fully understand them **By Dr. Paula Scalingi**

Senior leaders today face a confluence of technological, climate, and societal changes that are increasing the occurrence, intensity, and economic and human costs of natural and manmade disasters and events. These changes—developments and trends that have been evolving over the past two decades—are exacerbating and creating new threats and vulnerabilities. Feeding off each other, these changes pose challenges that transcend the traditional security mission space of prevention, protection, and deterrence to encompass resilience—preparedness, consequence mitigation, response, and recovery.

These changes include:

- Accelerating advances in electronics, computing, and other digital technologies that enable us to generate, record, process, transmit, receive and display massive amounts of information and distribute it to disparate recipients via a range of applications. These advances have permeated virtually every facet of how we live, creating a tightening web of interconnectivity from the global to individual levels, and opening new avenues for accidental disruptions and attacks.
- Climate-related changes, including extreme weather events and rising sea levels that can cause region-wide, largescale health and safety, economic, and environmental impacts.
- Growing urbanization and globalization of societies and ongoing innovations in social media and enabling technologies that allow rapid, real-time, 24×7 worldwide dissemination of information, disinformation, and rumor that can drive public reaction, political actions, and shift cultural norms.

We have yet to come to grips with the implications of these changes, or for that matter fully understand them. But they are transformational. Under certain scenarios, they have the potential to create a perfect storm impacting expanding urbanized regions that can include one or more major cities and hundreds of smaller cities, communities and special districts, encompass multiple counties, and cross-state and national borders. These "megaregions" have economies that in some cases surpass those of entire nations, and host thousands of commercial and non-profit enterprises, and industrial facilities that produce, store or use highly hazardous materials.

These megaregions are supported by a dense, interconnected network of critical infrastructures with concentrated areas of co-located critical assets. These infrastructures—utilities, communications, transportation and healthcare facilities, public safety and other government services, and other essential service providers with their supply chains are comprised of complex, integrated physical and cyber systems in a state of improvement with the incorporation of new "smart" technologies and other upgrades.

Many of these assets and the communities they serve are located along coastlines and vulnerable to sea-level rise and storm surge, in flood plains, along or on top of earthquake fault lines, and in areas with heavy vegetation, making them susceptible to high wind conditions and wildfires and heightening risk of direct or indirect disruption and damage from cyber and physical attacks, systems failures, and natural disasters.

At their most fundamental, these technological, climate and societal changes have injected new and unknown factors into the risk equation for infrastructures, businesses, and communities, altering how we need to assess and manage risk.

The Changing Risk Landscape

Technological Change Risk Factors -- Since the 1990s we have witnessed astounding strides in automation, communications, healthcare and other IT technologies and applications that have transformed the way we produce, deliver, and purchase goods and services; run our transportation systems; keep secure, safe and healthy; work, manage households, recreate, communicate, and socialize. Today we take the digital age in all its manifestations for granted, rely on, and in many cases are fully dependent on these technologies, and eagerly anticipate the next innovations in computing, communications, and other "smart" tools and systems that are improving our daily lives and how we do business.

The Smart City trend has grown quickly from a few large cities in Europe to major cities in the United States, including Boston, New York, Chicago, Seattle, San Francisco, and Charlotte, N.C., and to other cities, such as Melbourne, Australia, and Singapore.

Image Courtesy of IStock.com

» These megaregions are supported by a dense, interconnected network of critical infrastructures with concentrated areas of co-located critical assets. «

The stampede to develop Smart Cities technologies has been a natural outgrowth of the Digital Age. Smart Cities use IoT (Internet of things) sensors, actuators, and technology to connect components and analyze, control, and move large amounts of data across and among broad areas, connecting government agencies, infrastructures and other critical services, businesses, community services, and people to provide potentially unlimited benefits. The Smart City trend has grown quickly from a few large cities in Europe to major cities in the United States, including Boston, New York, Chicago, Seattle, San Francisco, and Charlotte, N.C., and other cities, such as Melbourne, Australia, and Singapore.

» The stampede to develop Smart Cities technologies has been a natural outgrowth of the Digital Age. «

Now many smaller cities are jumping on the bandwagon. Smart technologies are being marketed to operate lighting, automate buildings and security and access controls, manage water and wastewater systems, provide traffic information, operate intelligent energy grids, support law enforcement and emergency response, and push out a variety of public information. This has made Smart City technology a hot area of investment for national governments, technology firms, and research institutions who are increasingly partnering to launch new initiatives and start-ups.

The downside of the race to make our big cities and megaregions "smart" has made them increasingly vulnerable in four broad areas.

Cyber Attacks – These have steadily proliferated in type, targets, and level of sophistication since they emerged in the early 1990s as a security threat to critical infrastructures and government agencies. The focus has been largely on prevention and protection through developing cybersecurity tools, protocols, and standards, training work staffs and educating the public on ways to keep data safe, and development of technologies to counter attacks. In the last few years in a few major urban areas, such as Seattle, the focus moved beyond security to include cyber *resilience*—anticipating and mitigating damage and ways to respond and recover expeditiously, while limiting liability exposure, retaining customers, and managing public trust.

Today we are falling ever further behind in our abilities to thwart perpetrators, who range from recreational hackers to criminal gangs, nation-states, and non-state actors, who creatively use an ever-expanding variety of techniques—malware, Trojans, trapdoors and backdoors, web-based attacks, denial of service, phishing, botnets, and increasingly ransomware to target infrastructures, government agencies, healthcare facilities and insurers, major retailers, and financial institutions. Attacks are designed to steal, destroy, or corrupt data, cause service disruptions, hold data for ransom, and cause physical damage to process control systems and other critical components.

The Ninth Annual Cost of Cybercrime Study recently released by Accenture Security reports an increase of security breaches by 67 percent over the past five years with an 11 percent increase in 2018 over the previous year. The study attributes the increase to escalating cyber threats combined with new digital innovations that are being "churned out" faster than they can be secured.

Infrastructure Interdependencies – Potential impacts of interdependencies under different scenarios have been recognized as significant factors in regional security and resilience since the 2000-2001 Western Energy Crisis when there were multiple large-scale blackouts across California. Interdependencies often exist at multiple levels of increasing complexity, creating unexpected vulnerabilities. Incorporation of smart technologies adds additional layers of interconnectivity that can contribute to the severity of cascading impacts and complicate and prolong the restoration of services.

Systems Complexity – The addition of new smart technologies into existing integrated cyber and physical systems provides additional opportunities for inadvertent glitches and disruptions that can cause service loss and damage to sensitive electronic equipment and physical systems. Systems complexities also can be exploited by hackers, and state and non-state actors.

Smart Weaponry – UAVs are envisioned as the workhorses for Smart Cities, remotely monitoring and providing data on traffic, weather,

environmental conditions, supporting local law enforcement and emergency response, and delivering groceries, medicines, and other products to customers. They are already in use in some regions by local governments and utilities, and many others are exploring how drones with smart capabilities could be used. At the same time, localities are grappling with the potential for data compromise, privacy issues, and legal ramifications associated with drone use. Thus far, little attention paid to the use of drones as a weapon to physically target infrastructure, soft targets, or high population areas.

Climate Change -Related Risk Factors

In the past few years, we have seen a mind-numbing parade of extreme-weather events worldwide fueled by changing weather patterns. Many of these events have resulted in extensive damage to interdependent infrastructures and business and residential areas, with lengthy restoration periods. According to data from NOAA's National Centers for Environmental Information, the last two years have witnessed "historic" weather and climate disasters. There were 16 separate billion-dollar disaster events in 2017—three high category hurricanes, eight severe storms, two inland floods, a crop freeze, drought, and wildfires.

The combined cost was $306.2 billion. Last year, there were 14 disasters with each over a billion dollars in damages, with a total cost of $91.0 billion—additional wildfires, two major hurricanes, two hailstorms, three tornado outbreaks, two winter storms, two spring storms and drought in the southwest and southern plains. Extreme weather flood events are combining with rising sea levels to erode U.S. coastlines in the Carolinas, Florida, Louisiana, and California, putting infrastructure and communities at risk. Affected government agencies and private sector enterprises face costly decisions on the hardening or relocating critical assets, and other mitigation actions.

Societal Change-Related Risk Factors

Vast and rapid societal changes over the last two decades have transformed communities, cultures, beliefs and values, and influenced individual and collective political priorities. These changes have led to the globalization of societies and ideas and today largely determine what we eat, wear, buy, and where and how we live, work, and communicate and overall what is important to us. Driving these changes are the Internet, social media, and enabling technologies. Today we can have access to nearly unlimited information on virtually any topic, accurate or not, real or fake, from every conceivable source, in real-time. We can indeed have "tomorrow's news today", as the fictional evil media mogul Elliot Carver boasted to James Bond in the 1997 film *Tomorrow Never Dies*.

This is both a blessing and a curse for law enforcement, emergency responders, politicians, businesses, and other service providers that use social media and other smart communications technologies to push out and receive information for public information and marketing purposes. These tools can also be used to influence or inflame public opinion, discredit government agencies and businesses, and drive political decisions that may lead to unexpected consequences. At their most dangerous, these tools can be used by adversaries for disinformation, manipulation, and other means of subterfuge to sow dissent and foment political divisiveness, or to spark international conflict. They can also be used along with cyber-attacks for so-called "hybrid warfare" to wage a campaign against national infrastructures and populations short of using physical weapons. A primary target of hybrid warfare would be Smart Cities and Mega Regions.

Managing Risk in an Era of Change

The track record in improving security and resilience is mixed at best. In my 20 years working with thousands of cross-sector practitioners and experts in more than a dozen major metropolitan regions across the U.S. and Canada, I have seen significant strides made with limited resources: identification of dozens of gaps, improved plans and procedures, and development of tools and other capabilities. Some of these initiatives have taken root and grown over the years sustained by the original founding organizations and new members. At the same time, efforts to make progress have been frustratingly slow. Managing risk in an era of change requires a holistic approach that takes into account potential consequences from all threats and hazards, key physical and cyber assets, interdependences and system complexities, and potential impacts of technological, climate, and societal change.

There are federal directives that provide guidelines to address risk. This spring, the U.S. DHS Cybersecurity and Infrastructure Security Agency (CISA) unveiled a new approach centered on National Critical Functions to use as the basis of a prioritized Risk Registry with input from private sector critical infrastructures. Bob Kolasky, Assistant Director of CISA's National Risk Management Center, described this as a departure from the sector-specific approach that has been U.S. policy for the last 15 years to look at interdependency-related risk.

FEMA has updated its National Response Framework to emphasize coordination across critical infrastructure sectors and includes guidelines for stabilizing, repairing and restoring community lifelines.

It is unclear at this time how these revised national approaches can assist in developing risk strategies for Smart Cities, which must consider all-hazards vulnerabilities and consequences at the organizational and regional levels using unprecedented cross-sector coordination. According to Jim Wollbrinck, Manager of Security and Business Resiliency for San Jose Water Co. and a leader within the San Francisco Bay Area and the state on security and resilience initiatives, "Only a handful of cities are taking this cross-sector coordination seriously. Those cities that do so "tend to be unnoticed as this coordination is systemic. Since it works, events that would cripple other municipalities tend to have limited to no impact on these cities."

Constraints

Much of this slow progress is attributable to long-standing constraints. These include:

- Limited appreciation by elected officials, C-level leaders, and security managers of risks associated with organizational and regional interdependencies from threats and hazards.
- Cultural, competitive, legal, and security-related disincentives to look outside an organization to collaborate and team with other government and private sector organizations to improve regional security and resilience.
- Siloed functions, disciplines, and responsibilities, both within organizations and externally within supply chains, utilities, and other interdependent service providers.
- The sheer number and diversity of agencies and with roles, responsibilities, authorities, and interests in security, risk, and resilience.
- Challenges to developing and sustaining mechanisms to securely share information with external stakeholders for risk assessment and to support these efforts.
- Lack of access at the regional and local levels to interdependencies assessment capabilities, which are operated primarily by the national laboratories, universities, and other research institutions and chiefly produce analytical products for national policymakers.
- Inadequate investments by critical infrastructures and government agencies in security and resilience improvements, including providing necessary staff support and other resources.

The Safe City and Its Need for Interoperability

About the author:

Per Björkdahl is the Chair of the ONVIF Steering Committee

Many of us value individual safety, especially in cities. Physical security systems can deliver exactly that to citizens, though the management and operation of these systems can be challenging. Cities often use video management systems or other platforms to view and analyze camera footage in order to protect citizens and property, and to respond to events. They may also use intrusion, access control, building automation and fire detection systems, in conjunction with video surveillance.

Cities implementing this connected security approach have been dubbed 'safe cities.' Most safe cities share a common infrastructure and operate using sensors and/or cameras over a shared municipal network. Using these sensors and the data from many different devices synthesized through one interface, government officials and law enforcement are afforded a total, holistic view of a city's security.

Interoperability continues to present one of the greatest operational challenges in safe cities. The most common scenario is that municipalities have several different management systems for city operations that were created by different manufacturers, each with proprietary interfaces for integration. In order

What Senior Leaders Can Do

Ultimately, senior leaders will be the instrumental factor and force multiplier in ensuring the security and resilience of Smart Cities and Mega Regions in an era of change. There are a few low-cost and impactful steps that can be taken to overcome these constraints and mobilize and empower the development of risk management strategies to build secure and resilient Smart Cities and Mega Regions.

Internally within your organization:

- Integrate functions and personnel with responsibilities that span the security and resilience mission space. This can be accomplished by restructuring or setting up coordination mechanisms. Examples of typical functions include physical and IT security, emergency management, risk management, business continuity, chief resilience officers, and human resources and public affairs staff. Provide incentives for personnel to collaborate and undertake training in related functional areas outside their area of expertise.
- Elevate security and resilience to a top priority mission area and provide enabling staff and resources to develop and implement an enterprise-wide holistic risk strategy.
- Actively promote an internal culture of security and resilience that includes supply chains.

Externally:

- Become a security and resilience champion in the region where your company or agency's critical assets are located, and at the national levels within your sector and/or industry.
- Take on a leadership role in convening, or further developing an established regional public-private collaboration to develop and implement a risk-based regional security and resilience strategy. Provide resources to facilitate and administer it.
- Invite other senior leaders from all levels of government, critical infrastructures, and other key organizations to co-organize events and activities, including interdependencies exercises. Provide resources for staff to work with key stakeholders to identify and leverage capabilities and processes for secure cross-sector information sharing and assessing interdependencies.

About the author:

Dr. Paula Scalingi is Executive Director of the Institute for Innovating Security and Resilience and President of The Scalingi Group, LLC, which provides expertise on infrastructure security, regional resilience, and public-private partnership building for states and major metropolitan areas. Her extensive experience includes senior positions in government and the private sector and founding and directing two non-profits to build security and resilience capacities in the Pacific Northwest and San Francisco Bay Area. She also is an Adjunct Associate Professor at Georgetown University.

to connect its different systems together, cities often end up employing a "build once and maintain forever" approach, in which the continuing cost for integration of the city's systems becomes prohibitively expensive.

This is where the need for robust and well-defined standards comes into play. ONVIF has published several specifications and profiles for effective integration of devices and clients in the physical security industry, facilitating communication between technologies from different manufacturers and fostering an interoperable system environment. For Video Security systems, ONVIF has released *Profile S* for video streaming, *Profile T* for advanced video streaming and *Profile G* for storage and playback.

ONVIF has also released an export file format specification that outlines a defined format for effective export of recorded material and forensics, which has been adopted by both the U.S. National Institute of Standards and Technology, which makes technology recommendations for U.S. federal law enforcement agencies, such as the FBI, and the International Electrotechnical Commission.

In a safe city environment, the playback of video is important in responding to event types, but often incidents are recorded on multiple devices – both private and public. These files are typically exported in different proprietary formats, making it difficult for law enforcement to collect and analyze the video data, as demonstrated by the 2013 Boston Marathon bombing, where more than 120 FBI analysts reviewed in excess of 13,000 videos before discovering key evidence. The ONVIF Export File Format enables law enforcement as well as private users to more quickly and efficiently conduct forensic investigations using video of an incident from multiple sources.

These specifications together make it possible not only to integrate devices in multi-vendor video security system deployments in safe city environments but offer an effective common export file format that can streamline post-event investigations where authorities are trying to react as fast as possible.

As standards and industries collaborate even further and establish minimum interoperability standards together, the need for a multi-discipline physical security standard will become more urgent. ONVIF envisions that all physical security systems will eventually have the same interfaces for interoperability, and the organization is dedicated to facilitating the work of its members in developing such a multi-discipline standard.