ECONOMICS AND CULTURE 16(2), 2019

DOI: 10.2478/jec-2019-0026

SMART CITIES AND THE CHALLENGES OF CROSS DOMAIN RISK MANAGEMENT: CONSIDERING INTERDEPENDENCIES BETWEEN ICT-SECURITY AND NATURAL HAZARDS DISRUPTIONS

Busbach-Richard Uwe,[1] Gerber Brian J.[2]

[1]University of Applied Sciences Kehl, School of Public Administration,

Kehl – Germany, busbach@hs-kehl.de

[2] Arizona State University, Watts College of Public Service & Community Solutions, USA, Brian.Gerber@asu.edu

Abstract

Research purpose. Smart City technologies offer great promise for a higher quality of life, including improved public services, in an era of rapid and intense global urbanization. The use of intelligent or smart information and communication technologies to produce more efficient systems of services in those urban areas, captured under the broad rubric of "smart cities," also create new vectors of risk and vulnerability. The aim of this article is to raise consideration of an integrated cross-domain approach for risk reduction based on the risks smart cities are exposed to, on the one hand, from natural disasters and, on the other, from cyber-attacks.

Design / Methodology / Approach. This contribution describes and explains the risk profile for which smart cities are exposed to both natural disasters and cyber-attacks. The vulnerability of smart city technologies to natural hazards and cyber-attacks will first be summarized briefly from each domain, outlining those respective domain characteristics. Subsequently, methods and approaches for risk reduction in the areas of natural hazards and ICT security will be examined in order to create the basis for an integrated cross-domain approach to risk reduction. Differences are also clearly identified if an adaptation of a risk reduction pattern appears unsuitable. Finally, the results are summarized into an initial, preliminary integrated cross-domain approach to risk reduction.

Findings. Risk management in the two domains of ICT security and natural hazards is basically similar. Both domains use a multilayer approach in risk reduction, both have reasonably well-defined regimes and established risk management protocols. At the same time, both domains share a policymaking and policy implementation challenge of the difficulty of appropriately forecasting future risk and making corresponding resource commitments to address future risk. Despite similarities, different concepts like the CIA Triad, community resilience, absorption capacity and so on exist too. Future research of these concepts could lead to improve risk management.

Originality / Value / Practical implications. Cyber-attacks on the ICT infrastructure of smart cities are a major vulnerability – but relatively little systematic evaluation exists on the topic. Likewise, ICT infrastructure is vulnerable to natural disasters too – and the risk of more severe natural disasters in the context of a global trend toward massive cities is increasing dramatically. Explicit consideration of the issues associated with cross-domain integration of reduction of interdependent risk is a necessary step in ensuring smart city technologies also serve to promote longer-term community sustainability and resilience.

Keywords: smart cities; risk reduction; disasters; IT-security; natural hazards; cybersecurity; risk management

JEL codes: Q55; M15.

Smart Cities and the Challenge of Complex and Interdependent Risk

In the last ten years or so, "Smart City" projects have become more common across national settings. A long-term global trend towards greater urbanization – steady increases in densely populated urban areas – has necessitated a response for the need to support a higher quality of life in cities, including improved public services. The use of intelligent information and communication technologies (ICT) to produce more efficient systems of services in those urban areas, which can be captured under the rubric of "Smart

Cities" offers the promise of enabling the linkage of high technology, greener environmental practices with lower adverse impacts and a greater overall well-being for urban residents. However, the exact nature of complex risk and vulnerabilities occurring across a broad range of critical infrastructure and other key systems in a smart city context is a question generally not developed robustly by most discussions of performance effectiveness. Cyber-attacks on the ICT infrastructure of a smart city are widely recognized as a major potential vulnerability. But there is relatively limited systematic evaluation used to minimize community-scale risk associated with such attacks. And beyond cyber-attacks, it is also important to recognize the ICT infrastructure that underpins the efficient operation of services expected by citizens and businesses is also subject to disruption from natural hazards.

Risk and vulnerability associated with natural hazards are dramatically increasing not only because of the global climate change but also because the trend towards intense urbanization—including megacities often located in coastal areas that are subjected to higher risk of disruption. This means a greater natural hazard risk exposure to the global population in the aggregate, which in turn increases the level of risk for disruption of ICT infrastructure in a smart city setting.

Though risk reduction is an established construct in disaster management, the new challenges of cross-domain or interdependent risks associated with the development of smart cities are not sufficiently understood at present. The topic of how risks in domains such as natural hazards might also affect the levels of risk in the domain of smart ICT has not been addressed explicitly to date. Risk management related to ICT infrastructure is often a separate silo from risk management related to natural hazards even though smart technologies are related to key infrastructure systems (e.g., transportation, emergency response services) that are affected by natural hazard disruptions. And of course, natural hazards (e.g., floods, extreme weather, drought) can adversely affect the operations of smart ICT. This is the straightforward proposition of cross-domain or interdependent risk. Further, it seems likely that risk management of both ICT infrastructure and other critical physical infrastructure would benefit by the assessment of potential interdependencies between disruption to smart systems from both human sources (e.g., hacking) or natural hazards sources (e.g., extreme weather) in order to build and improve the capacity of Smart Cities to serve an overall risk reduction imperative in densely populated urban environments. What is not so clear is the best way to assess and manage such cross-domain risk interdependencies.

As a result, the aim of this article is to raise consideration of the potential for an integrated cross-domain approach for risk reduction based on the risks smart cities are exposed to, on the one hand, from hazards disruptions in the ICT technical domain, such as cyber-attacks, and on the other, from disruptions to ICT systems arising from natural hazard risk and vulnerability. The vulnerability of smart city technologies to natural hazards and cyber-attacks will first be summarized briefly from each domain, outlining those respective domain characteristics. Risk dependencies and cascading risk situations are also considered. Subsequently, methods and approaches for risk reduction in the areas of natural hazards and ICT security will be examined in order to create the basis for an integrated cross-domain approach to risk reduction. Differences are also clearly identified if an adaptation of a risk reduction pattern appears unsuitable. The result is a preliminary consideration of a possible integrated approach for risk reduction as a component of smart cities systems and suggestions for further research to operationalize the assessment of such an integrated risk management approach for a Smart City setting.

Defining the Concept of Smart Cities

First, we begin with the basic notion of what constitutes a so-called Smart City, given the various uses of that term. From our perspective, "smart" in the context of identifying or describing a smart city, or smart city systems, may be seen as having three key elements. One key feature of "smartness" is the efficient provision of services for citizens and businesses. The city is increasingly composed of networked, digitally-enabled devices directly embedded into the fabric of cities (e.g., smart meters, transponders, sensor networks, software-controlled equipment) that produce continuous streams of data that dynamically feed into management software and control rooms enabling the real-time regulation of city systems to provide more efficient services in, for example, transport management, energy supply, emergency services and so on. These are supplemented by new media such as smartphone apps that both

present a range of information about the city and generate data about its citizens such as location and activity. Connecting, integrating and analyzing the data produced by these various forms of ubiquitous computing and digitally instrumented devices provides a more cohesive and smart understanding of the city that enhances the efficiency and sustainability (Hancke et al., 2013; Townsend 2013). Furthermore, the rich seams of data can be used to better depict, model and predict urban processes and simulate the likely outcomes of future urban development (Schaffers et al., 2011; Batty et al., 2012).

A second element of smartness in this context is the idea that urban policy, development and governance are improved by the modern ICT infrastructure allowing for reconfiguration of human capital, creativity, innovation, education, participation, sustainability, and administration (Caragliu et al., 2009). A smart city utilizes e-government, publishes open data and fosters an open data economy, creates citizen-centric dashboards about city performance, encourages citizen participation in reporting issues and planning, enables urban test-bedding wherein companies can try new technologies for improving urban services, actively nurture start-up companies and promote the use of ICT in education programs.

A third element in the use of the smart city construct emphasizes the use of digital technologies and ICT to promote a citizen-centric model of urban development and management that promotes social innovation and social justice, civic engagement and transparent and accountable governance (Townsend 2013). A smart city thus promotes a smart society that provides equal opportunities, serves local communities, and reduces inequalities. Participatory planning and community development, open source platforms, software and data, freedom of information and digital and data literacy are basic ideas in this conception of a smart city.

Although these three elements are recognized as appropriately related to the use of the smart city construct, they are also sufficiently distinct from one another that they might not be utilized simultaneously when the term is applied in a given case. Whatever the nuances of usage, the key is that these elements all are rooted in the same framework: a continually available, networked technical infrastructure that continuously provides data whose evaluation serves to control and improve urban life.

While this is a reasonable approach to defining the use of the smart city term as referring to several critical dimensions, it is also important to note one essential characteristic or dimension that is lacking from most standard approaches to the concept. It is difficult to speak of "smartness" in cities and their essential systems without addressing the question of whether such systems simultaneously serve to reduce risk and promote sustainability in the aggregate. That is, it is important for smart city approaches to include not only the efficient provision of services in a city but also to likewise include risk reduction as a macro-level goal essential to smartness along with attention to efficient precautions for essential risks such as disruption to essential services through cyber-attacks or natural hazards. This lack of attention to coupling smart city approaches for risk reduction is an important omission in the field because of the simultaneous trends of globalization increases urbanization and increases natural hazards vulnerability. Thus, it seems imperative that the essential goals of a smart city approach – livability, efficiency, equity – should be understood as likely to be realized only to the extent that those same systems contribute to the promotion of community resiliency and reduced risk.

Because suitable conceptualization of integrated risk management seem to be lacking in terms of current discourse on smart cities – approaches to disaster risk reduction and ICT security are generally treated as separate domains – we offer preliminary thoughts here on why and how greater attention can be paid to the necessary linkages of both in practice.

Smart Cities, ICT, Natural Hazards and Risk and Vulnerability

The standard definition of risk used in the world of practice and research in the area of crisis or disaster management is to think of risk as being a function of the probability of a disruption occurring weighted by the potential adverse impact from the hazard on human safety, on the built environment (infrastructure comprising a community), on human systems that permit a community to function, and/or on natural environmental systems. A hazard itself can be thought of as generally consisting of items (e.g., a natural phenomenon like extreme weather, human actions, such as hacking or terrorism) that are capable of acting against some type of asset in a manner that can result in harm. For example, a flood is

a natural hazard and a hacker (or the activity of hacking) can be thought of as a hazard as well. The key consideration is that threats apply the force (water, wind, exploit code, etc.) against an asset that can cause a loss event to occur. Though there are some common characteristics in thinking of cyber and natural hazards, each category has its unique or specific characteristics, which will be discussed below.

Vulnerability and resulting risks from natural hazards: While hazards such as various forms of extreme weather and seismic activity are natural; a crisis or a disaster itself is, as many have noted, a social phenomenon that results from human decisions and actions (Quarantelli, 2000; United Nations, 2010). Among other things, this means that the adverse effects of a disaster are not evenly distributed across a community. This basic insight calls attention to the idea of social vulnerability to disaster, defined by Bankoff (2006) as: "Social systems generate unequal exposure to risk by making some people more prone to disaster than others and these inequalities are largely a function of the power relations (class, age, gender and ethnicity among others) operative in every society." A body of research on disasters and crises has recognized these considerations and offers explication of various dimensions of social vulnerability (Thomas, et al., 2013).

Vulnerability and resulting risks to cyber-attacks: In general terms, three categories of vulnerabilities can be distinguished: availability, integrity, confidentiality. These three together are referred to as the security CIA triad (Perrin, 2008). If a system suffers loss of confidentiality, then data has been disclosed to unauthorized individuals. This could be high level secret or proprietary data, or simply data that someone wasn't authorized to see. For example, if an unauthorized employee is able to view payroll data, this is a loss of confidentiality. Similarly, if an attacker is able to access a customer database including names and credit card information, this is also a loss of confidentiality.

Loss of integrity means that data or an IT system has been modified or destroyed by an unauthorized entity. This could be the modification of a file, or the change in the configuration to a system. For example, if a file is infected with a virus, the file has lost integrity. Similarly, if a message within an email is modified in transit, the email has lost integrity. Availability ensures that data and systems are up and operational when they are needed. Or said in another way, loss of availability indicates that either data or a system is not available when needed by a user. For example, if a Web server is not operational when a customer wants to purchase a product, the Web server has suffered a loss of availability. Since the information technology infrastructure of a smart city implements highly distributed systems, all the "classic technical" vulnerabilities of distributed systems appear here as well: messages can be lost in the network system, pure bandwidth or overloading respectively, administration/operating of networks, the need to interface primarily incompatible information technology systems, denial of Service attacks etc. (Harinath et al., 2017).

If smart cities are defined in such a way that the focus is on smart delivery of smart services, availability is obviously one of the most essential problems regarding the vulnerability of the information technology infrastructure. Here, the highly complicated information systems themselves, the high degree of networking of the components and the volume of data (Townsend, 2013) are to be mentioned above all. In addition, there is the special circumstance that the information technology systems of the individual participants in the provision of Smart Services – electricity supplier, water supplier, local public transport, city and county administration – must be highly integrated in order to be able to offer their services really smartly.

The primarily incompatible information technology systems of the different actors have to be connected to each other partly via proprietary interfaces. As these are a multitude of information technology systems, the number of interfaces tends to be very high. Firstly, each interface itself is a potential point of attack. Secondly, the high number of interfaces often leads to a loss of overview as to which interface has which relevance or function. This problem is exacerbated by the fact that the documentation of information technology systems is often inadequate due to time pressure and a lack of resources. Very often, source code is regarded as the best resource for software maintenance (Garousi et al., 2015). In the event of an attack, this may lead to the situation that no rapid countermeasures can be taken even when identifying the point of attack. Understanding source code is usually more difficult than reading normal documentation.

Loss of data integrity, for example, through corruption in the context of cyber-attacks, can have a

massive impact on all three approaches, as one can define the term smart city. First of all, erroneous data can cause serious problems in the availability of IT infrastructure. This would affect the first concept of the term smart city. The second concept focuses more on the use of data to continuously improve a city's services and, if necessary, control them in real time. At the technical level, manipulated data can lead to reduced performance or, under certain circumstances, impair the availability of services. On an administrative or political level, manipulated data can lead to faulty decisions that seriously impair the coexistence in an urban society.

The third perspective on the term smart city is affected by the problem of data corruption. Transparent and accountable governance plays a central role in the model of citizen-centered development and administration. Threats to the credibility of politicians, administrative staff or citizens' movements through manipulated data represents serious risk of undermining the basic principles and concepts of a smart city. Such risk is to not only to the data, but it is a type of political integrity in democratic governance is adversely affected as well. This security category of confidentiality influences the development of a user-centric city too. Lack of confidentiality violates privacy. Although open data platforms aim at transparency and accountability in open urban societies with democratic governance, this does not imply in any way that individual citizens prefer or support public exposure of otherwise private data. In other words, data corruption due to cyber-attacks or abuses within a public sector administrative system represented a threat of diminished trust in government. The plausible net effect of the loss of both confidentiality and data integrity is a loss in the perceived political integrity of governance systems that undergird smart city efforts.

Integrated, Cross-Domain Risk Management

Disaster risk reduction: There are well-established international efforts aimed as disaster risk reduction and overall management improvement. The major doctrine on disaster risk reduction, from an international perspective (rather than a specific nation state), is best summarized by three key documents produced under the auspices of the United Nations: the Yokohama Strategy in 1994, the Hyogo Framework in 2005, and the Sendai Framework for Disaster Risk Reduction in 2015 (see de la Poterie & Baudoin, 2015; Ray-Bennett, et al, 2020 for descriptive summaries of the three frameworks). Doctrine in the area of natural hazards and disasters has emphasized the promotion of coordination between organizations across and between governmental and nongovernmental sectors—and key organizations within of course. To summarize, the trend over the last several decades in numerous countries has been to move beyond narrower command and control response systems (oriented toward post-incident management) and towards more proactive systems of mitigation, risk reduction, and cross-sector coordination and collaboration.

In terms of defining the basic concept of disaster risk reduction, the UNISDR (2009, p. 10) provides the elements constituting it in practice: "the concept and practice of reducing disaster risk through systematic efforts to analyze and manage the causal factors of disasters, including through reduced exposure to hazards, lessened vulnerability of people and property, wise management of land and the environment, and improved preparedness for adverse events." Efforts aimed at reducing risk have the effect of contributing to community resilience. Again relying on the UNISDR (2009, p. 24) for a basic definition, resilience is explained as: "the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions."

Risk minimization in ICT: A closer look at the area of risk minimization ICT field reveals that this is a multi-level approach. In order to achieve confidentiality, integrity and availability, measures must be implemented in the technical, organizational and management areas. With regard to management, operational, analytical and executive levels are affected.

At the lowest level, technical measures are taken to ensure ICT security. This includes, for example, the physical security of data transmission, encryption, access control, availability networks of servers using redundancy, and so on. A closer look reveals that this lowest level is subdivided. One distinction relates to the possible involvement of end users, who must actively authenticate themselves, for example, in

access control. A further distinction is made between the various ICT disciplines that implement the security measures. While the physical security of data transmission is arranged in the network area, the conception of availability networks of servers is located in the architectural design area, before it is transferred to the server administration area after implementation. Already here, it becomes apparent that IT security is a complex topic. Even at the lowest implementation level, different groups of people and ICT disciplines are involved, which can only achieve risk minimization through interaction.

On the second level, which addresses organizational issues, a collection of ICT security patterns was created (Yoder et al., 1997; Fernandez-Buglioni, 2013) to minimize complexity and apply coherent and useful solutions. The model approach was originally developed in the field of architecture (Alexander, 1977) and initially adapted for ICT in the field of software engineering (Gamma, 1994). The selection of ICT security measures for implementation is facilitated by these IT security patterns. However, unlike the patterns in software engineering, IT security patterns lack both a model system that categorizes patterns by purpose and context and a model language that addresses the dependencies between patterns to minimize more complex IT risks.

The third level, which addresses management issues, is often associated with the concept of information risk management. The term information indicates that the use of data in the work context and its value for the work context are addressed. On the other hand, the term management shows that ICT security is not only a technical issue, but also – or above all – a management task. On this level, there are approaches that essentially consist of a collection of methods and processes. Organizational and normative aspects are addressed.

ISO/IEC 27005 emphasizes the process perspective but does not recommend or even name any specific risk management method (ISO/IEC 2018). It does implies that it is a continual process consisting of a structured sequence of activities, some of which are iterative: establishing the risk management context, quantitatively or/and qualitatively assess, treat, keeping stakeholders informed throughout the process and monitor and reviewing risks, risk treatments, obligations and criteria on an ongoing basis, identifying and responding appropriately to significant changes. In contrast to ISO/IEC 27005, the Risk IT framework (ISACA 2009) is more comprehensive because it complements ISACA CobiT (ISACA 2019), which provides a comprehensive framework for the control and governance of business-driven information technology solutions and services. While CobiT already provides a set of controls to mitigate IT risk, Risk IT Framework complements this approach with a set of procedures to identify, control and manage ICT risks across the enterprise. All in all, this results in a very comprehensive, holistic approach.

This is the goal of the Framework for Improving Critical Infrastructure Cybersecurity des National Institute of Standards and Technology too (NIST2018). The Framework is a risk-based approach to manage cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business/mission drivers and cybersecurity activities. The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sector presenting industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Implementation Tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Framework Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. In a sense, it is the most comprehensive approach as it combines methods and approaches of the Center for Computer Security, the National Institute of Standards and Technology, the CobiT approach, the International Society of Automation and the ISO standard. In addition, the concept of profiles places a clear focus on the operational implementation in the respective organizations.

Even if these theoretical approaches are manifold, the following statement often applies to the practical implementation:

"The information security community does a great job of identifying security vulnerabilities in individual technologies and penetration testing teams help secure companies. At the next level of scale, however, things tend to fall apart" (Conti, et al., 2015).

What are the reasons for these implementation problems? Within the multi-level approach regarding ICT security, the two lowest levels – the concrete ICT security measures and the ICT security patterns – lack a process-oriented, integrational view to support the implementation of the described measures in organizations. The management-oriented third level addresses information risk management. However, it is doubtable whether the proposed frameworks overcome this lack of process orientation and integration. The problems that occur when implementing new processes and changing organizational structures is not considered in a serious way. Change Management methods are not integrated into the frameworks; they are missing. Furthermore, anti-patterns in policy-making in the area of cybersecurity implementations are normally not reflected (Busbach-Richard, 2019).

Looking at smart cities in particular, additional aspects with respect to IT risk management have to be taken into account. Firstly, it can be said that each city is unique in terms of their corporate network. Secondly, there is the need to provide a 24/7 availability. And thirdly, a large city easily has 30 or more administrative units that place different business demands on IT, and consequently, on IT security. These requirements often compete with each other (Hayslip, 2016). In many cases, the administrative units do not see the overall task that a city should fulfil, but only its isolated area. This can be named as silo perspective. The dependencies are understood only to a very limited extent. In order to resolve this, communication, coordination and mediation between individual administrative units is absolutely necessary. There might be no optimal solution with regard to risk management with respect to competing requirements.

Integration of Approaches to Risk Management: Nussbaum (2014) argues that "while the risk assessment community has been involved in the trial and error application of various risk models to various problems, there have been some difficulties with attempting to use models like these to look at sector and jurisdiction level risks." The key issue, according to Nussbaum, is related to scale and/or scope. Traditional risk assessments are oriented toward either a specific (i.e., single) system or singular or discrete tasks. This suggests that there are nontrivial challenges in translating risk assessment to a very complex set of both operational relationships (in a system or systems context) and complex governance relationships in the case of an entire urban area with multiple jurisdictional authorities (e.g., other adjacent cities, counties and/or other regional authorities, provincial or state authorities and national government authorities. Such considerations are core to the challenge of pursuing an integration of risk management strategy and practical approach for joint or interdependent risk between locally-prevalent natural hazards and ICT systems that undergird smart cities.

Likewise, it is important to understand at least four categories of challenges associated with, and as potential drivers of, interdependent risk. First, communication problems are a definitional characteristic of any crisis situation; that applies here as well. Second, discrete operational silos exacerbate the management of comprehensive risk. Likewise, stakeholders from different disciplines make coordinated efforts difficult. And lastly, pure policy patterns present essential challenges in the form of short term reaction versus long term strategic planning for risk reduction.

When the challenge of addressing cross-domain assessment, that is, reducing silos in assessment and management, and of addressing long-term strategic planning over interdependent risk, we can think of such efforts as an integrated risk management approach. In practice, this means several things. First, explicit assessment of systems' interactions are required in order to measure and understanding how to define operational vulnerabilities and mitigate associated risks. Second, potential cascade points of failure also need to be defined and measured in order to produce appropriate risk mitigation strategies. Third, it is necessary to develop explicit communication mechanism on layers, ICT systems and stakeholders.

While the scope or scale of the challenges listed above are fundamentally important, it is also helpful to recognize a basic similarity of risk management in the two domains of ICT security and natural hazards. Both domains use a multilayer approach in risk reduction, both have reasonably well-defined regimes and established risk management protocols, and importantly, the fundamental concepts used in both

areas are similar. This promises a degree of potential consonance as approaches to establishing smart city systems. Table 1 highlights this potential for consonance or a future of more fundamentally integrated risk management practices. The table notes similarity in key concepts, a relatively similar set of policy challenges and administrative approaches, and some degree of similarity in operations' practices—even though the administrative and operational systems of the two domain are quite different, of course.

Table 1 highlights the proposition that similar challenges have to be overcome in risk minimization in both ICT security and natural hazards management. Cross-organizational coordination across several levels and between different governmental and non-governmental institutions requires defined, but at the same time flexibly changeable interfaces. The attempt to systematically minimize or reduce risks can be found in both ICT risk management and disaster management. And at the same time, both domains share a policymaking and policy implementation challenge of the difficulty of appropriately forecasting future risk and making corresponding resource commitments to address future risk. Despite certain similarities in otherwise separate risk management domains, the challenge is to investigate areas that could lead to new findings to improve risk management integration between the domains. For instance: Can the CIA Triad provide new insights in the context of broader disaster management? How can key concepts of community resilience, hazard mitigation, absorption capacity in the natural hazards domain translate to useful practices in ICT security?

Table 1. Comparisons in Smart City ICT and Natural Hazards Risk Management

Common Organizing Concepts	*Key Concepts: Natural Hazards Domain*	*Key Concepts: ICT Domain*
Risk reduction Risk minimization Operational efficiency Cross-sector governance	Disaster Risk Reduction (DRR) for natural hazards hazard mitigation, community resilience, absorption capacity (for disruptions)	CIA-Triad: Confidentiality, integrity and availability
Common Policy Challenges	*Administrative Considerations*	*Current Approaches*
- level of scale dysfunctionality - imbalance between resources to meet protection needs and underlying extant vulnerabilities - challenges in producing long-term strategic risk management - span of control: explicit public sector responsibilities versus private property ownership and control of private resources	- disaster management systems designed to accommodate increasing scale – difficult to resource appropriately in practice - ICT: risk management systems are designed to solve problem at hand. Scaling is rarely addressed - ICT: Short term reaction in favor of long term strategic planning	- International and national disaster response and recovery frameworks, with DRR emphasis - ICT risk management: ISACA CobiT
Common Challenges in Operations	*Operations Needs*	*Current Approaches*
- cross-organizational interface - risk assessment and communication - systematic efforts to analyze risks comprehensively - Focus on either a specific system or a discrete task	- required for both ICT protection and NH risk management - defined, but at the same time flexibly changeable interfaces	- Separation of technical (operational), organizational and management level - DRR practices for natural hazards; ICT security practices - Natural hazards: routine assessment; - ICT: penetration tests, routine assessment; ISO/IEC 27005

Conclusions

This article represents a brief, preliminary statement on a complex challenge. Its basic premise is that as communities attempt to develop a comprehensive smart city status, or attempt to deploy a set of what might be considered smart city systems, attention should be paid to a broad range of interdependent risks. Because risks associated with natural hazards, such as heat, drought, flooding, cyclones, or other extreme weather, pose a broad set of important challenges to densely populated urban areas, the challenge for smart city systems is to integrate tradition ICT security efforts as part of a broader integrated risk management strategy for a community (or larger national governance systems). This seems straightforward, but as discussed above, a considerable degree of complexity is involved in operationalizing this premise. However, if smart cities are to be smart in terms of real-world efficacy, then risk reduction strategies should strive to be integrated across domains in order to maximize community resilience—and community resilience should be incorporated as a central value of smart cities, along with efficiency, equity and livability concerns.

Such an imperative means a close and coordinated exchange of risk management information and practice between those in the ICT domain and those in the traditional natural hazards management domain. Such an integration of risk management practice and coordination of resources and effort is also likely to depend on the development of research agendas motivated by this theme. Existing research literatures on measuring and assessing risk interdependencies should be expanded to consider how, in a context of intense global urbanization and the emergence of smart cities' systems, the linkage between ICT infrastructure and built physical infrastructure, and the new vectors of risk that emerge from those systems' exchanges.

In order to achieve the goal of an integrated risk management strategy, it appears necessary to analyze and understand common policy challenges such as "level of scale dysfunctionality", "lack of visibility in politics and public" for the prevailing risks in order to find suitable bases for an efficient, targeted and solution-oriented governance strategies. Similarly, straightforward applied research on how key public and private sector practitioners and systems of governance contribute to, or inhibit development of, comprehensive risk management integration. In terms of governance, assessment of governmental and nongovernmental organizational interactions is necessary to understanding the potential efficacy of both structural and non-structural risk mitigation practices. In terms of key practitioners, understanding how those public sector agencies charged with responsibility for critical infrastructure protection complete their tasks is needed—along with how cross-sector coordination with their private sector counterparts functions in practice.

Ultimately, the central challenge is to promote awareness of cross domain risk and how more comprehensive integrative risk management strategies and governance regimes can promote efficient, livable, equitable and resilient communities, if they are to be considered "smart" in a meaningful sense.

References

Alexander, C. (1977). A Pattern Language: Towns, Buildings, Construction. Oxford: University Press.

Andress, J. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Amsterdam: Syngress.

Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A.,Bazzani, A., Wachowicz, M., et al. (2012). Smart cities of the future. European Physical Journal Special Topics, 214 (1), 481–518

Birkmann, J. J., & von Teichman, K. (2010). Integrating disaster risk reduction and climate change adaptation: Key challenges—scales, knowledge, and norms. *Sustainability Science*, *5*(2), 171–184.

Busbach-Richard, U. (2019). The Case of IT-Security: Anti-Patterns in Policy Making and its Implementation. Book of Abstracts of the First International Conference on Sustainable Development in Business and Economics. Skopje: IBI/IBF.

Caragliu, A., Del Bo, C., and Nijkamp, P. (2009). Smart Cities in Europe. Series Research Memoranda 0048. Amsterdam: VU University Amsterdam, Faculty of Economics, Business Administration and Econometrics.

Conti, G., Cross, T., Raymond, D. (2015). Pen Testing a City Retrieved from https://www.blackhat.com /docs/us-15/materials/us-15-Conti-Pen-Testing-A-City-wp.pdf on September 24th 2019.

De la Poterie, A. T., & Baudoin, M. A. (2015). From Yokohama to Sendai: Approaches to participation in international disaster risk reduction frameworks. *International Journal of Disaster Risk Science*, *6*(2), 128–139.

Essays, UK. (2018). The Importance Of Security In Distributed Systems Information Technology Essay. Retrieved from https://www.ukessays.com/essays/information-technology/the-importance-of-security-in-distributed-systems-information-technology-essay.php?vref=1 on September 24th 2019.

Garousi, G., Garousi-Yusifoglu, V., Ruhe, G., Zhi, J., Moussavi, M., & Smith, B. (2015). Usage and usefulness of technical software documentation: An industrial case study. Information and Software Technology, 57, 664–682

Fernandez-Buglioni, E. (2013) Security Patterns in Practice: Designing Secure Architectures Using Software Patterns. Hoboken: Wiley Publishing

Gamma, E., Helm. R., Johnson, R. & Vlissides, J. (1994). Design Patterns (the Gang of Four book). Boston: Addison-Wesley.

Garousi, G., Garousi, V., Ruhe, G., Zhi, J., Moussavi, M., & Smith, B. (2015). Usage and usefulness of technical software documentation: An industrial case study. *Information & Software Technology, 57*, 664–682.

Hancke, G. P., de Carvalho e Silva, B., & Hancke, G. P, Jr. (2013). The role of advanced sensing in smart cities. Sensors, 13 (1), 393–425.

Harinath , D., Satyanarayana , P. (2017). A Review on Security Issues and Attacks in Distributed Systems. Journal of Advances in Information Technology, 8 (1), 1–9.

Hayslip, G. (2016) What I have learned as CISO for a Smart City. Retrieved from https://www.linkedin.com/ pulse/what-i-have-learned-ciso-smart-city-cissp-cisa-crisc-ccsk?articleId=6099504343512272896#comments-6099504343512272896&trk=prof-post on September 24th 2019.

ISACA (2009). The Risk-IT-Framework-Excerpt. Retrieved from https://m.isaca.org/ Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf on September 26th 2019.

ISACA (2019). COBIT 2019 Publications & Resources. Retrieved from http://www.isaca.org/ COBIT/Pages/ COBIT-2019-Publications-Resources.aspx on September 26th 2019.

ISO/IEC (2018). ISO/IEC 27005:2018 - Information technology - Security techniques - Information security risk management (third edition). Retrieved from https://www.iso27001security.com/ html/27005.html on September 26th 2019.

Mijalkovic, Sasa & Cvetković, Vladimir. (2013). VULNERABILITY OF CRITICAL INFRASTRUCTURE BY NATURAL DISASTERS.

NIST (2018). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf on September 26th 2019.

Nussbaum, B. (2014). The 'Levels of Analysis' Problem with Critical Infrastructure Risk. In Journal of Physical Security, 7(1), 43–50.

O'Rouke, T.D. (2007). Critical infrastructure, interdependencies and resilience. The Bridge Vol. 37 No. 1, 22–29.

Perrin, C. (2008). The CIA Triad. Retrieved from https://www.techrepublic.com/blog/it-security/the-cia-triad/ on September 24th 2019.

Ray-Bennett, N. S., Mendez, D., Alam, E., & Morgner, C. (2020). Inter-agency collaboration in natural hazard management in developed countries. In B. J. Gerber (Ed.), *The Oxford encyclopedia of natural hazards governance*. New York, NY: Oxford University Press.

Robert, B., Morabito, L., Cloutier, I., & Hémond, Y. (2015). Interdependent critical infrastructures resilience: Methodology and case study. *Disaster Prevention and Management*, *24*(1), 70–79.

Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson,M., & Oliveira, A. (2011). Smart cities and the future internet: Towards cooperation frameworks for open innovation. J. Domingue, et al. Eds.), Future Internet Assembly pp. 431–446. LNCS: Springer.

Townsend, A. (2013).Smart cities: Big data, civic hackers, and the quest for a new utopia. New York: W.W. Norton & Co.

Thomalla, F., Downing, T., Spanger Siegfried, E., Han, G., & Rockstrom, J. (2006). Reducing hazard vulnerability: towards a common approach between disaster risk reduction and climate adaptation. *Disasters*, *30*(1), 39–48.

Thomas, D. S., Phillips, B. D., Lovekamp, W. E., & Fothergill, A. (2013). *Social vulnerability to disasters*. Baton Roca, FL: CRC Press.

United Nations. (2010). *Natural hazards, unnatural disasters: the economics of effective prevention*.

UNISDR (United Nations International Strategy for Disaster Reduction). (2009). *2009 UNISDR terminology on disaster risk reduction*. Geneva, Switzerland: United Nations.

Yoder, J. , Barcalow, J. (1997). Architectural patterns for enabling application security. In Proceedings of the 4th Conference on Patterns Languages of Programming (PLoP'97).