Evaluating User Experience Considerations for Emergency Responders in the Age of Smart Cities

Katelynn A. Kapalo[1,2], Joseph J. LaViola Jr.[1],
University of Central Florida[1]
Brown University[2]
kate.kapalo@knights.ucf.edu

Joseph A. Bonnell
Phoenix Fire Department[3]

Abstract
The cyber landscape continues to evolve regularly due to the convergence of information technology (IT) and operational technology (OT). IT/OT convergence refers to the concept that real-time data collected is merged with the systems that monitor and drive organizations' operational aspects, creating a new way in which industry and enterprise organizations must operate. As we see this convergence across the industry, it has been brought to light in the context of Smart Cities. Smart Cities are generally defined as urban environments that leverage aspects of ubiquitous computing and sensors to collect real-time data that is leveraged to improve citizens' quality of life. Because of the convergence of OT and IT and the ever-changing landscape of technology, first responders will eventually have access to building information, sensor data, and fire protection system data in real-time. However, these technologies pose risks due to a general lack of awareness and validation surrounding standards in infrastructure and security of Smart Cities. This paper aims to analyze the extant literature to develop a taxonomy of first responder user experience needs in the context of Smart Cities.

Keywords: Smart Cities, Emergency Response, Public Safety, Cybersecurity, Privacy, Data Collection, User Experience

Introduction

The cyber landscape continues to evolve regularly due to the convergence of information technology (IT) and operational technology (OT) (Heritage, 2019). IT/OT convergence refers to the concept that real-time data collected is merged with the systems that monitor and drive organizations' operational aspects, creating a new way in which industry and enterprise organizations must operate. As we see this convergence across the industry, it has been brought to light in the context of Smart Cities. Smart Cities are generally defined as urban environments that leverage aspects of ubiquitous computing and sensors to collect real-time data that is leveraged for the purpose of improving the quality of life for citizens (Kitchin, 2015; Nel & Nel, 2019)

Because of the convergence of OT and IT and the ever-changing landscape of technology, first responders will eventually have access to building information, sensor data, and fire protection system data in real-time. However, these technologies pose risks due to a general lack of awareness surrounding standards in infrastructure and security of Smart Cities (Srinivasan, 2016). The goal of this paper is to

[1] 4000 Central Florida Boulevard, Orlando, Florida, 32816, USA
[2] 184 Hope Street, Providence, RI, 02912, USA
[3] 200 W. Washington Street, Phoenix, AZ, 85003, USA

analyze the extant literature to develop a taxonomy of first responder needs in the context of Smart Cities.

Related Work

Since September 11, 2001, the United States has transitioned homeland security strategies to include an all-hazard response (Bullock et al., 2013). This transition to all-hazards changed the methods and ways we handle emergency response today in the United States and has further-reaching consequences beyond just the United States. As computing advancements have occurred, we are connected now more than ever before. Thus, as threats evolve, so must our strategies for mitigating those threats. Formative work in this area has included research on the impact of different emerging technologies such as wearables, virtual/augmented reality, and artificial intelligence on emergency response and crisis management (Dugdale et al., 2019).

The Changing Landscape of Public Safety

In addition to physical threats, cyber threats are becoming increasingly more common. Critical infrastructure, such as utility and water management companies are now facing more risks due to adversaries' ability to disrupt larger agencies and increase their impact through further-reaching interference. At first glance, this does not seem to impact emergency response directly; however, when you consider the architecture of Smart Cities as a whole, it is essential to consider these threats due to their impact on public health and the ability for emergency responders to safety deploy assets for search and rescue.

To illustrate the importance of critical infrastructure on public health in the event of a cyberattack, we can leverage the water and waste management industry as an example. Water and waste management influence the ability of cities to operate normally. Historically, water usage was measured manually through meter readings, requiring labor to come out to homes and businesses and measure water use through indicators on the water supply. The movement to smart meter systems reduces costs associated with the workforce but introduced a new attack vector through the internet protocol (IP) addresses of these meters (Al-Ali & Aburukba, 2015; Jiménez-Buendía et al., 2015). Adversaries can gain access to usage, disrupting, and distracting from their overall goal to bring infrastructures down (Bulbul et al., 2015). Because waste removal and contaminated water impact quality of life and health, these kinds of cyberattacks transform from a cyber issue to a public health issue. Therefore, the landscape of public safety in the context of Smart Cities introduces new challenges, not only for cybersecurity professionals and officials but also for the first responders who may need to manage and treat citizens without access to fully functioning infrastructure systems (Huang et al., 2007). Thus, bringing down the utilities of a city magnifies existing vulnerabilities and puts society and citizens at risk. This is because it creates an environment in which first responders and the city’s emergency response system cannot successfully operate, posing new challenges by compounding problems even further, allowing adversaries to maximize the damage.

In a similar vein, it is critical to evaluate the impact of building structure in the context of Smart Cities. As we continue to build and renovate existing structures, we must also evaluate building construction. This involves a discussion greater than just standards and codes alone due to the evolving and dynamic nature of incident response. For example, more recent work in this area demonstrates the need for architects and developers to assess the impact of design on building evacuation to better support occupants in the event of fire or earthquake emergencies (Arbib et al., 2019). Therefore, by incorporating all necessary stakeholders in the planning process of new construction, we ensure that disaster and emergency response concerns are addressed in a way that is not only aesthetically pleasing but functionally supports emergency situations. This will become an increasingly dire problem as construction practices continue to evolve.

Emergency Response and the Impact on Critical Infrastructure

The introduction of Smart Cities raises some interesting questions regarding what the impact will be on incident response. As we integrate more technologies, our communities are more connected than ever before. This integration and connectivity of technology can positively influence emergency response as a whole. For example, dispatchers may be able to send pictures from callers to the first responders before they arrive on the scene. In specific use-cases, this could mean the difference between life or death for a victim of a car accident or other trauma because these first responders can access information about the car make and model, thus increasing the time they spend rescuing the victim and reducing the time it takes to make critical and tactical decisions about the extrication of the victim. This decrease in time allows for enhanced decision making and awareness, but it also affords the opportunity for multiple stakeholders to build a more comprehensive operational picture.

Alsamhi et al. (2019) proposed that the Internet of Things (IoT) for public safety can be conceptualized as different aspects of emergency management requiring sensors and data that may or may not overlap, depending upon function areas. Based upon this framework, crime control, and traffic control may overlap in the sense that sensors used in both of these areas could be feeding information to first responders who may be securing an incident scene, or who may have had to conduct a traffic stop, but ended up dealing with an escalated situation in which the suspect tries to evade law enforcement.

Some research in this area has focused on the introduction of new frameworks, models, and systems to predict, detect, and counter disasters (Boukerche & Coutinho, 2018). The literature is divided on what is the most effective way to model disasters and to formulate effective response plans, but most research converges on the idea that disasters require a different framework than what is already afforded by Smart Cities due to interruptions in connectivity and denial of resources (Boukerche & Coutinho, 2018). Therefore, in order to respond to disasters and manage risk in Smart Cities, several challenges must be addressed to ensure that Smart Cities are protected and able to effectively mobilize emergency response in the unfortunate event of a disaster or emergency scenario.

Challenges and Opportunities Related to Incident Response

Before we can begin to understand the impact of cyber threats on Smart Cities, it is vital that we look at the existing threat vectors to determine if there are existing vulnerabilities that can be mitigated through either best practices or existing means of risk assessment and management. For example, we have general knowledge regarding what types of threats and vulnerabilities exist when discussing location-based and mobile data. Based on this information and our existing knowledge of emergency response systems, it is known that first responders rely on mobile devices to receive information. With the introduction of Smart Cities, these mobile devices will only increase in number. To truly understand potential threats, it is critical to identify any existing gaps in the framework of current systems and to integrate this known data into mitigation strategies.

Srinivasan et al. (2016) outlined some of the most critical factors to consider in terms of designing the emergency response ecosystem within Smart Cities. For instance, firewalls typically protect data in centralized data centers. However, in the event of an emergency, this system is not convenient, nor does it facilitate effective mobilization of emergency response. This is because any structure created for immediate or emergency access in this system could be leveraged as an attack vector (Srinivasan, 2016). Infrastructure as a service (Iaas) seems to represent the best possible solution since resources can be accessed on-demand from the centralized data centers, but even these solutions have shortcomings due to the reliance on a centralized system.

Method

We conducted a search using publications related to Smart City initiatives between the years of 2005 and 2019. The year 2005 was chosen as a starting point since Cisco first began announcing their efforts towards investigating the feasibility of smart cities around that time (Swabey, 2012). A few years later, IBM released its plans for smart city initiatives during the recession (Cavada et al., 2014). The process involved one iteration and was conducted between June and July 2020. We conducted the search via Web of Science and Science Direct. The search terms were derived from keywords used in

combination such as: “emergency response and smart cities,” “smart cities and emergency department,” “smart cities and disaster response,” “emergency response and security,” and “digital city emergency.” For the purposes of our literature review, articles must have met two criteria to warrant inclusion:

1. Published between the years 2005 and 2019
2. Involved discussion of Smart Cities and Cybersecurity in the broader context of emergency response and incident management

We excluded articles and works that covered topics outside the scope of the emergency response. The search terms identified over 500 papers, but only a select sample are included in this analysis for relevance. Thematic analysis was conducted to determine what the highest priority areas are in terms of connecting cybersecurity risks to emergency management. Based on the findings, we capture major themes from the literature in the analysis section below.

Analysis and Results

Based on the themes in the extant literature, we captured the impact of Smart Cities on emergency response in terms of three key areas within cybersecurity: privacy, data management, and architecture. Each of these three main focal points involves cybersecurity implications that every organization and stakeholder must evaluate before attempting to integrate emergency response into the Smart City infrastructure. These key areas and their definitions are captured in Table 1 and described in further detail below.

Table 1. Core Areas for Cybersecurity Concerns in the Context of Emergency Response for Smart Cities

Key Areas Within Cybersecurity	Definition
Privacy	Refers to the general concept that citizens have a right to selectively choose how information is shared about them (Elmaghraby & Losavio, 2014; Zoonen, 2016)
Data Collection and Management	Refers to the types of data captured, stored, and retrieved to monitor threats in Smart Cities. However, this also may include indicators that demonstrate how successful a Smart City initiative is (Marsal-Llacuna et al., 2016)
System Architecture	Refers to the hardware, software, and other components that make up the Internet of Things (IoT) in the Smart City infrastructure (Alsamhi et al., 2019).

Privacy

The literature review resulted in numerous articles that described privacy as one of the leading concerns when considering smart cities' impact on emergency response (Srinivasan, 2016). Interestingly, this area emerged as an area of interest for both the citizens first responders serve and the first responders/agencies themselves. Drawing from some of the examples presented in the literature, Martínez-Ballesté et al. (2013) captured the importance of distinguishing five different types of privacy in the context of Smart Cities. For example, a utility company might collect sensor data for utility usage. Still, they may want to correlate that with other services (such as natural gas usage or telecommunications services) to provide more attractive commercial services (Martínez-Ballesté et al., 2013). This example illustrates the importance of transparency and privacy controls. If citizens feel

like their daily lives are being monitored, there may be less trust in government agencies. More importantly, it may create conflict between commercial entities who do not want to share data due to commercial advantages. Despite this, some citizens may not feel that this type of data collection infringes on their privacy or rights. However, it is difficult to argue that location-based data should be perceived on a similar level. In more tangible terms, location-based data also raises concerns regarding privacy (Elmaghraby & Losavio, 2014), (Srinivasan, 2016). If citizens' and first responders' locations are tracked, this opens up the opportunity for people to potentially leverage this data in nefarious ways.

Based on what we know regarding location-based services, awareness of a persons' location data could result in physical and cybersecurity issues. If adversaries can access the system, this could result in further mass casualty incidents, communications jamming, and potential disruptions to existing plans. Location-based information is particularly critical for active shooter scenarios or mass casualty incidents. If adversaries can access location-based data, there is an opportunity to disrupt the channels through which first responders communicate, rendering their plans to rescue victims and neutralize the shooter useless (Huang et al., 2007).

Data Collection and Management

In considering the impact of Smart Cities and IoT data, we cannot ignore the impact of data collection and the implications for storing, managing, and retrieving data to analyze the impact of cyber risks. Because this is such a critical part of keeping information secure, it will become necessary for city officials to understand and maintain several key components to ensure that data is being used appropriately and that vulnerabilities are not introduced. More importantly, it will also become critical for first responders working in the field who need reliable data and information about the status of the applications and systems they rely upon to manage emergencies.

Security Information and Event Management (SIEM)

Trusted vendors represent a critical component of supply chain management in terms of emergency response and security. The purpose of SIEM is to manage and monitor data to identify potential problems and threats. However, security managers and cybersecurity professionals may not feel comfortable setting up their systems to share data beyond the local level due to the potential for leakage of sensitive information. This problem is compounded further through the introduction of Smart Cities to the existing data collection procedures. The implementation of Smart Cities implies that there will be a surplus of information and data to capture, store, retrieve, and analyze. Therefore, it becomes necessary to have a plan in place regarding how to store this information securely. More importantly, if there is a need to share local data at the state or federal levels, then it becomes even more essential for organizations to develop plans that incorporate interoperability standards to share data across and between agencies.

Deep Fakes

Data visualization is a defining feature of Smart Cities and Internet of Things sensors (IoT) (Matheus et al., 2020). Now more than ever before, first responders will access information in real-time. However, the critical factor to understanding and interpreting this data will be the transparency through which it is obtained. First responders do not have the same needs as citizens. Therefore, their interactions with data and the systems used to present and display this data in Smart City environments requires careful analysis (Citron & Chesney, 2019). Because decisions must be made so quickly, it is important to acknowledge the impact of transparency on emergency responders' ability to rapidly consume information for successful incident response (Matheus et al., 2020). Thus, transparency from both government agencies to responders plays a critical role in understanding how this information will impact citizens. When considering our approach to counterterrorism and related homeland security issues, this seems to be one of the areas where cybersecurity is critical for understanding the impact of falsified data and data that has been manipulated or tampered with (Citron & Chesney, 2019).

Overall, when discussing data collection and data management, it is apparent that citizen perceptions of the data's trustworthiness and transparency will be paramount (Matheus et al., 2020). Likewise, it

will be necessary for first responders to trust the information they are receiving is accurate and verified. Khan et al. (2020) developed methods for ascertaining and correlating camera-based surveillance data in Smart Cities. This kind of research provides a path forward for identifying techniques and strategies that can help verify and validate whether or not the information is real or if it has been manipulated.

System Architecture

To properly assess risk, system architecture must be initially designed with risk mitigation strategies in place. Additionally, the system architecture is critical for understanding where vulnerabilities may exist and how to mitigate the impact of cyber threats. For this reason, it is essential to evaluate the vital components of the system architecture.

Human-Computer Interface (HCI)

Understanding the impact of human behavior on systems has been a critical part of evaluating the impact of system architecture on the security of Smart Cities (Hyman et al., 2019; Singh et al., 2015) However, in the context of public safety, the human-computer interface, sometimes referred to as the human-machine interface, plays a direct role due to the room for error. While it is critical to examine how interfaces support professionals managing risk, it becomes even more critical for first responders working in the field (Kapalo et al., 2019). First responders not only deal with time pressure, but they also must manage fatigue, increased workload, and other human performance problems when on the scene of an active incident. For these reasons, emergency management stakeholders must factor in the human-machine interface aspect of system architecture to improve the user experience of emergency responders working within Smart Cities.

Device Management Protocols, Redundancy, and Unidirectional Gateways

Often in discussing cybersecurity risks, we conceptualize the connectivity and availability of devices as the core issue. Ginter (2013) proposed the idea that connectivity is not necessarily the overarching problem. However, when thinking about these issues in the context of Smart Cities, it is possible to mitigate threats and patch vulnerabilities through the intentional design of device management protocols. This research provided evidence that the use of unidirectional gateways should become more widespread. The idea is to minimize the impact of the network exposed central processing units (CPUs) by making them expendable. By leveraging principles of separation, critical infrastructure is protected because the integrity of the internal CPUs is maintained without compromising the system (Ginter, 2013a). Therefore, it is unnecessary to reduce the connectivity of the devices, but it is more critical to ensure that separation is maintained.

Additionally, Soyata et al. (2019) described a redundant system that leverages mesh networks in multiple modes to help support both normal operations and more critical operations in the event of disasters and crises. By managing systems and creating this separation, we can build more resilient cities. More importantly, it is possible for devices to be managed so that they are not used as weapons against the community.

Drones and Other Emerging Technologies

For the most part, the discussion thus far has emphasized the importance of infrastructure architecture. However, part of the issue lies in the connections and signals between the infrastructure of a Smart City and the devices and sensors used to collect the data. Because of this, we are seeing more issues than ever before concerning communications and electronics jamming. While this problem has existed in the defense domain for many years, relatively recently have we seen threats related to communications jamming in disaster response.

One way an attack can occur is through the devices and sensors that collect the data for us. So instead of manipulating the data, an adversary may choose to leverage local networks to disrupt communications. Unmanned aerial vehicles (UAVs), also referred to as drones, emerged as a potential point of vulnerability in Smart Cities. Since drones often rely on wireless networks and unencrypted hardware, researchers have successfully demonstrated how simple it can be to conduct cyberattacks

and hijack this technology-based upon known protocols and manufacturer nuances (Vattapparamban et al., 2016).

Because of the active role drones play in understanding the Internet of Things (IoT) for Public Safety, this issue will define the efficacy of drone programs and their delivery of real-time information in the event of a crisis (Alsamhi et al., 2019). On the one hand, drones allow us to conduct several activities such as communication (e.g., temporary hot spots), surveillance, and rescue missions to support public safety agencies (Vattapparamban et al., 2016). However, as much as drones can be used to support first responders and other public safety officials in the field, several issues create vulnerabilities and allow attackers access to emerging technologies connected to the broader Smart City ecosystem. For example, while drones are generally used to collect information for situational awareness, it is possible for attackers to interfere with drone systems and (Kharchenko, Vyacheslav Torianyk, 2018; Vattapparamban et al., 2016). Using this information as a foundation, we can better secure technologies such as UAVs by recognizing and identifying vulnerabilities and coming up with solutions to prevent and mitigate attacks.

Despite these vulnerabilities, Kim et al. (2012) developed novel ways to leverage jamming attack nodes to disrupt an attack in progress. These methods must be accessible to the community and incorporated into technology standards to prevent attacks on the sensors that help us collect the data. For this reason, we must continue to be vigilant and develop new methods such as this to leverage first responder networks. As such, this relates to our discussion on data management as well. Without reliable information, first responders cannot leverage the existing data to provide a better picture of the incident.

Discussion and Future Research Directions

Taken together, these three core areas identified in the literature search represent the importance of understanding first responder perspectives when implementing Smart City infrastructures. By focusing on the needs of emergency response, we can support first responders and their ability to continue to protect and serve their communities. Too often, cybersecurity focuses on an overall reactive approach. Once a threat is identified, it is logged, and incident response teams become responsible for managing and mitigating damage. However, from a review of the literature and further analysis of these concepts, it is apparent that a reactive approach will not be enough to manage the inherent risks that Smart Cities pose to the emergency response infrastructure. To identify vulnerabilities and manage risk, city officials, public safety officials, and other relevant stakeholders must take proactive steps to prevent adversaries from creating situations that cannot be contained through traditional means.

In summary, from what we know in the extant literature, we must support emergency response by protecting the emergency response infrastructure from information instead of attempting to secure the existing data. When we consider cybersecurity at the baseline level, we typically conceptualize it as protecting sensitive data. While we do not refute that this is important, the underlying strategies for homeland security in the future must consider the influence of newly emerging technologies and the evolving attack vectors. While we can appreciate the benefits of a society with access to new information and data sources, we also must recognize the challenge of avoiding adversaries who might leverage threats in new ways. By staying vigilant and implementing security standards, we can ensure that citizens and the first responders serving them are protected, even in a connected world.

Conclusion

Based on the literature review, we identified several key areas where relevant stakeholders and city officials will need to address the impact of cyber threats on emergency response, specifically within the context of smart cities. This paper aims to highlight the key areas where stakeholders, citizens, and cybersecurity professionals must focus attention to protect critical infrastructures. By predicting threats and identifying vulnerabilities before attacks occur, we can increase the efficacy of our security measures to protect our first responders and the citizens they serve.

Acknowledgments

This work was performed **in part** under the following financial assistance award, 70NANB18H160, from the U.S. Department of Commerce, National Institute of Standards and Technology (NIST). The views expressed in this dissertation are the views of the author and participants' alone and do not represent the official views of the U.S. Government, the University of Central Florida, or any fire department. Certain commercial entities, equipment, materials may be identified in order to describe a concept or experimental procedure adequately. Use of company names or devices does not imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor is it intended to imply that the entities, materials, or equipment are the best available for the purpose. This paper is dedicated to the memory of Chief Winston Minor.

References

Al-Ali, A. R., & Aburukba, R. (2015). Role of Internet of Things in the Smart Grid Technology. *Journal of Computer and Communications*, *9*(3), 229–233.

Alsamhi, S., Ma, O., Ansari, M., & Gupta, S. (2019). Collaboration of Drone and Internet of Public Safety Things in Smart Cities: An Overview of QoS and Network Performance Optimization. *Drones*, *3*(1), 13. https://doi.org/10.3390/drones3010013

Arbib, C., Arcelli, D., Dugdale, J., Moghaddam, M., Arbib, C., Arcelli, D., Dugdale, J., Moghaddam, M., Emer-, H. M. R., Arbib, C., Arcelli, D., Dugdale, J., & Muccini, H. (2019). Real-time Emergency Response through Performant IoT Architectures To cite this version : HAL Id : hal-02091586 Real-time Emergency Response through Performant IoT Architectures. *International Conference on Information Systems for Crisis Response and Management (ISCRAM)*.

Boukerche, A., & Coutinho, R. W. L. (2018). Smart Disaster Detection and Response System for Smart Cities. *IEEE Symposium on Computers and Communications*, *August*. https://doi.org/10.1109/ISCC.2018.8538356

Bulbul, R., Sapkota, P., Ten, C.-W., Wang, L., & Ginter, A. (2015). Intrusion Evaluation of Communication Network Architectures for Power Substations. *IEEE Transactions on Power Delivery*, *30*(3), 1372–1382.

Bullock, J. A., Haddow, G. D., & Coppola, D. P. (2013). *Introduction to Homeland Security: Principles of All-Hazards Risk Management*.

Cavada, M., Hunt, D. V. L., & Rogers, C. D. F. (2014). *Smart Cities : Contradicting Definitions and Unclear Measures . Smart Cities : Contradicting Definitions and Unclear Measures*. *June*, 0–13. https://doi.org/10.13140/2.1.1756.5120

Citron, D. K., & Chesney, R. (2019). Deep Fakes : A Looming Challenge for Privacy , Democracy , and National Security. *107 Calif. L. Rev. 1753*.

Dugdale, J., Negre, E., & Turoff, M. (2019). ICT and Artificial Intelligence for Crisis and Emergency Management. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 626–628.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities : Safety , security and privacy. *Journal of Advanced Research*, *5*(4), 491–497. https://doi.org/10.1016/j.jare.2014.02.006

Ginter, A. (2013a). Securing industrial control systems: ICSs are vulnerable targets to cyber attacks. More than conventional IT-security solutions are needed to protect them. *Chemical Engineering*, *120*(7).

Ginter, A. (2013b). Unidirectional Security Gateways: Stronger Than Firewalls. *Proceedings of ICALEPCS*.

Heritage, I. (2019). Protecting Industry 4.0: challenges and solutions as IT, OT and IP converge. *Network Security*, *2019*(10), 6–9. https://doi.org/10.1016/S1353-4858(19)30120-5

Huang, Y., He, W., & Nahrstedt, K. (2007). Requirements and System Architecture Design Consideration for First Responder Systems. *2007 IEEE Conference on Technologies for Homeland Security*, 39–44. https://doi.org/10.1109/THS.2007.370017

Hyman, B., Alisha, Z., & Gordon, S. (2019). Secure Controls for Smart Cities: Applications in Intelligent Transportation Systems and Smart Buildings. *International Journal of Science and Engineering Applications*, *8*(6), 167–171.

Jiménez-Buendía, M., Ruiz-Peñalver, L., Vera-Repullo, J. A., Intrigliolo-Molina, D. S., & Molina-Martínez, J. M. (2015). Development and assessment of a network of water meters and rain

gauges for determining the water balance. New SCADA monitoring software. *Agricultural Water Management*, *151*, 93–102. https://doi.org/10.1016/j.agwat.2014.11.013

Kapalo, K. A., Wisniewski, P., & Laviola, J. J. (2019). First In , Left Out : Current Technological Limitations from the Perspective of Fire Engine Companies. *International Conference on Information Systems for Crisis Response And Management*, *May*, 1286–1299.

Khan, P. W., Byun, Y.-C., & Park, N. (2020). A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in. *Electronics (MDPI)*, *9*(3), 484. https://doi.org/10.3390/electronics9030484

Kharchenko, Vyacheslav Torianyk, V. (2018). Cybersecurity of the Internet of Drones : Vulnerabilities analysis and IMECA based assessment. *The 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT*, 364–369.

Kim, Y. S., Mokaya, F., Chen, E., & Tague, P. (2012). All Your Jammers Belong To Us - Localization of Wireless Sensors Under Jamming Attack. *IEEE International Conference on Communications (ICC)*, 949–954.

Kitchin, R. (2015). Making sense of smart cities: Addressing present shortcomings. *Cambridge Journal of Regions, Economy and Society*, *8*(1), 131–136. https://doi.org/10.1093/cjres/rsu027

Martínez-Ballesté, A., Pérez-Martínez, P. A., & Solanas, A. (2013). The Pursuit of Citizens ' Privacy : A Privacy-Aware Smart City Is Possible. *IEEE Communications Magazine*, *June*, 136–141.

Matheus, R., Janssen, M., & Maheshwari, D. (2020). Data science empowering the public : Data-driven dashboards for transparent and accountable decision-making in smart cities. *Government Information Quarterly*, *37*(3), 101284. https://doi.org/10.1016/j.giq.2018.01.006

Nel, D., & Nel, V. (2019). Governance for Resilient Smart Cities. *International Council for Research and Innovation in Building and Construction (CIB)*, *July*.

Singh, P., Garg, S., Kumar, V., & Saquib, Z. (2015). A Testbed for SCADA Cyber Security and Intrusion Detection. *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC, August*, 1–6. https://doi.org/10.1109/SSIC.2015.7245683

Soyata, T., Habibzadeh, H., Ekenna, C., Nussbaum, B., & Lozano, J. (2019). Smart City in Crisis : Technology and Policy Concerns Smart city in crisis : Technology and policy concerns. *Sustainable Cities and Society*, *50*(June), 101566. https://doi.org/10.1016/j.scs.2019.101566

Srinivasan, R. (2016). Privacy Conscious Architecture for improving. *2016 Smart City Security and Privacy Workshop (SCSP-W)*, 1–5. https://doi.org/10.1109/SCSPW.2016.7509559

Swabey, P. (2012). IBM, Cisco and the business of smart cities. In *Information Age*.

Vattapparamban, E., Güvenç, İ., Yurekli, A. İ., Akkaya, K., & Uluağaç, S. (2016). *IWCMC 2016 : the 12th International Wireless Communications & Mobile Computing Conference : September 5-9, 2016, Paphos, Cyprus*. 216–221.

Zoonen, L. Van. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472–480. https://doi.org/10.1016/j.giq.2016.06.004