

Nataliia Neshenko
Elias Bou-Harb
Borko Furht

Smart Cities: Cyber Situational Awareness to Support Decision Making

 Springer

Smart Cities: Cyber Situational Awareness to Support Decision Making

Nataliia Neshenko • Elias Bou-Harb • Borko Furht

Smart Cities: Cyber Situational Awareness to Support Decision Making

 Springer

Nataliia Neshenko
Boca Raton, FL, USA

Elias Bou-Harb
San Antonio, TX, USA

Borko Furht
Boca Raton, FL, USA

ISBN 978-3-031-18463-5 ISBN 978-3-031-18464-2 (eBook)
<https://doi.org/10.1007/978-3-031-18464-2>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2022

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The challenges in urbanization forced worldwide governments and industries to embrace the smart city vision. A modern urban infrastructure no longer operates in isolation but instead leverages the latest technologies to collect, process, and distribute aggregated knowledge to improve the quality of the provided services and promote the efficiency of resource consumption. However, this technological development manifests in the form of new vulnerabilities and a plethora of attack vectors. The ambiguity of ever-evolving cyber threats and their debilitating consequences introduce new obstacles for decision-makers. Therefore, cyber situational awareness of smart cities emerges as a mission-critical task that requires novel strategies for practical and prompt decision-making. By synthesizing the body of existing knowledge on cyber incidents, detection, and cognition methods, this book strives to advance the adoption and deployment of corresponding strategies in the realms of smart cities.

This book overviews the drivers behind the smart city vision, describes its dimensions, and introduces the reference architecture. It further enumerates and classifies threats targeting the smart city concept, links corresponding attacks, and traces the impact of these threats on operation, society, and the environment. Besides, it introduces a data-driven situational awareness, provides an in-depth description of the respective solutions, and highlights the prevalent limitations of these methods. More importantly, the book points out promising research directions and emphasizes the demand and challenges for developing holistic approaches to transition these methods to practice to equip the user with extensive knowledge regarding the detected attack instead of a sole indicator of ongoing malicious events. To this end, the book introduces a cyber situational awareness framework that can be integrated into smart city operations to provide timely evidence-based insights regarding cyber incidents and respective system responses to assist decision-making.

What Is Covered in This Book?

Our goal is to cover the topics from the motivation behind smart cities to defining its essential elements to studying cybersecurity threats and building a foundation for cyber situational awareness using data-driven methods and deep learning algorithms. This book is divided into two parts. Part I magnifies the motivation and significance of the concept of smart city (Chap. 1) and its particular challenges concerning cybersecurity (Chap. 2). Part II studies situational awareness methods that address elements of smart city technologies (Chap. 3), defines situational awareness programs, and offers the corresponding framework for ICS deployed in critical infrastructure (Chap. 4) and its particular case - water facilities (Chap. 5). Chapter 6 points out research directions and stresses the demand and challenges for developing holistic strategies and techniques to enforce cyber situational awareness methods in practice. Each chapter in the book can stand alone, defining a particular aspect of smart city or cyber situational awareness for it. There is a sequence in each chapter that builds on the previous one to provide a conceptual understanding of the smart city concept and detailed cybersecurity threats coupled with an approach for getting started with building cyber situational awareness.

Chapter 1: Rise of Smart Cities

Facing the socioeconomic challenges in urbanization, worldwide governments and industries embrace the smart city concept and establish transformation projects that demonstrate tremendous growth. These projects combine information and communication technologies to engage and integrate citizens, visitors, and business communities into an intelligent ecosystem to support better decision-making and cocreating solutions for urban issues. This engagement positively shifted essential city operations toward sustainable, effective, and efficient functions. This chapter strives to shed light on the drivers behind the concept and sets the scene for the smart city by providing its definition, separating building blocks, and highlighting contemporary technological advances.

Chapter 2: Cyber Brittleness of Smart City

This chapter shifts the focus on the cyber fragility of the smart city concept, elaborates on fundamental peculiarities of smart city cybersecurity, and raises awareness regarding past real-world cyber incidents that affected smart cities. It examines prevailing threats targeting smart cities that are identified from actual and potential cyberattacks.

Chapter 3: Cyber Situational Awareness Frontier

Cyber situational awareness or network security awareness is a vital component of a holistic view of cybersecurity. This chapter puts forward a new perspective on sustained cyber situational awareness for smart cities. It explores monitoring and attack detection methods to support the perception of cyber awareness. Further, it examines risk assessment methods and contextualized threat intelligence, which

enable the characterization and anticipation of advanced and coordinated threats via assessing their possibilities and impact. Finally, the chapter explores the strategies that model dependencies among smart cities' components to clarify how threats affect the entire ecosystem.

Chapter 4 Cyber Situational Awareness for Industrial Control Systems (ICS) Deployed in Smart City

The increased number of cyberattacks against critical infrastructure, in particular, their vulnerable network-assessable automated control systems, paved the way for new approaches to defining cyber situational awareness and forensic methods for smart cities. This chapter defines the activities required to enforce a sound situational awareness program and elaborates on design challenges that hinder the transition to operation in ICS realms. This chapter introduces a framework to integrate into operation to enhance situational awareness by providing evidence-based insights about ongoing cyber incidents and respective system responses to assist decision-making.

Chapter 5: Case Study: Situational Awareness for Water Treatment Systems

Cyberattacks on water systems can cause significant damage to the ICS equipment and render chemical or biological hazards, which can have social and financial implications. This chapter recaps the history of cyber incidents against water systems and conveys the significance of cyber situational awareness in this environment. To this end, this chapter offers a business case for applying the cyber situational awareness framework to the small-scale water treatment plant, similar to those found in small cities.

Chapter 6: Looking ahead: Future Perspectives and Opportunities of Cyber Situational Awareness for Smart City

Smart cities worldwide suffer from rapidly evolving cyber threats and attacks that exploit advanced heterogeneous technologies. Thus, failing to manage these cyber threats impairs the trustworthiness of smart cities' endeavors. Although research and operational communities are actively developing the methods to address this imperative task, numerous observations require attention. This chapter encapsulates several issues on sustained cyber situational awareness for smart cities and elaborates on several possible research directions to address these topics.

Boca Raton, FL, USA
San Antonio, TX, USA
Boca Raton, FL, USA
January 2022

Nataliia Neshenko
Elias Bou-Harb
Borko Furht

Contents

Part I Cybersecurity of Smart City

1 Rise of Smart Cities	3
1.1 Forces of Change	3
1.2 Set the Scene for Smart City	7
1.2.1 What Make City Smart?	8
1.2.2 Dimensions of Smart City	9
1.3 Summary	15
References	15
2 Cyber Brittleness of Smart Cities	19
2.1 Cybersecurity of Smart Cities vs Enterprise IT Security	19
2.2 Cyber Incidents: Decades in Retrospect	20
2.2.1 The Colonial Pipeline Attack	21
2.2.2 Israel’s Water System Attack	22
2.2.3 Onslow Water and Sewer Company Hack	23
2.2.4 Battle of City Atlanta	23
2.2.5 Kemuri Water Company	24
2.2.6 Ukraine Power Grid Attack	24
2.2.7 German Steel Mill Attack	25
2.2.8 The Cyber-Attack on Saudi Aramco	25
2.3 Adversary Model	26
2.3.1 Attackers	26
2.3.2 Impact of Cyber-Attacks	27
2.3.3 Categorization of Cyber Threats	29
2.4 Summary	36
References	37

Part II Cyber Situational Awareness for Smart City

3 Cyber Situational Awareness Frontiers	43
3.1 Toward Analytics-Driven Situational Awareness	43

3.1.1	Data Analytical Techniques	45
3.1.2	Threat Perception: Attack Detection Methods	49
3.1.3	Evaluation Metrics	51
3.1.4	Threat Comprehension: Risk Analysis and Cyber Threat Intelligence	53
3.1.5	Risk Analysis	55
3.1.6	Cyber Threat Intelligence	57
3.1.7	Threat Projection: Strategies for Modeling Cascading Effect	61
3.2	Analytics-Driven Cyber Situational Awareness for Smart City: Are We There Yet?	65
3.2.1	Toward Threat Coverage	65
3.2.2	Toward Human Cognition Engagement	65
3.2.3	Toward Data Availability	67
3.3	Summary	68
	References	72
4	Cyber Situational Awareness for Industrial Control Systems (ICSs) Deployed in Smart City	77
4.1	Development of Successful Situational Awareness Program	77
4.1.1	Plan for Situational Awareness	78
4.1.2	Collect and Analyze Relevant Data	78
4.1.3	Communicate to Make Appropriate Decisions	79
4.1.4	Enhance Process and Technology	79
4.2	Framework Overview	80
4.2.1	Design Considerations	80
4.2.2	Detailed Design	84
4.3	Continuous Improvement: Evaluation Strategy	101
4.4	Summary	103
	References	104
5	Case Study: Situational Awareness for Water Treatment Systems	107
5.1	History of Attacks Against Water Infrastructure	107
5.1.1	Israel's Water System Attack	107
5.1.2	Onslow Water and Sewer Company Hack	108
5.1.3	Kemuri Water Company	108
5.1.4	The Maroochy Water Services Attack	109
5.2	Cyber Situation Awareness for Water Treatment Plant	109
5.2.1	Cyber-Physical Process Overview	109
5.2.2	Dataset Overview	112
5.2.3	Operational Patterns Examination	113
5.2.4	Cyber Incident Detection	114
5.2.5	Anomaly Localization	115
5.2.6	Interactive Visualization	117
5.3	Summary	121
	References	122

6 Looking Ahead: Future Perspectives and Opportunities of Cyber Situational Awareness for Smart Cities	125
6.1 Challenges and Future Perspective	125
6.2 Summary	128
References	129

Part I

Cybersecurity of Smart City

” *Great results can be achieved with small forces.*
— **Dalai Lama**

Chapter 1

Rise of Smart Cities



Facing the socio-economic challenges in urbanization, worldwide governments and industries embrace the smart city concept and establish transformation projects that demonstrate tremendous growth. These projects combine information and communication technologies to engage and integrate citizens, visitors, and business communities into an intelligent ecosystem to support better decision-making and co-creating solutions for urban issues. This engagement positively shifted essential city operations toward sustainable, effective, and efficient functions. The application of smart technologies and data harnessing methodologies developed numerous solutions to cities' key challenges (including rapid urbanization, increased homelessness, rise in crime, climate change, and more). From improving traffic conditions to optimizing energy consumption, smart cities enhance the quality of life of their residents by reducing carbon emissions while optimizing utility costs. This chapter strives to shed light on the drivers behind the concept and sets the scene for the smart city by providing its definition, separating and elaborating on each building block, and highlighting contemporary technological advances.

This chapter first overviews the challenges of modern cities in Sect. 1.1 and sets the scene for the smart city concept in Sect. 1.2 by providing a definition and exploring its dimensions from architectural, technological, economic, and social perspectives. Finally, Sect. 1.3 concludes the chapter.

1.1 Forces of Change

Despite the global pandemic and ongoing wars, the world's population is rapidly increasing; it has almost reached 8 billion as of May 2022 [4]. With the immense growth, the world witnessed an increasing concentration of residents in the cities: more than half the world's population currently lives in urban areas (Fig. 1.1), and the trend is projected to continue. Accordingly, the United Nations predicts that two-

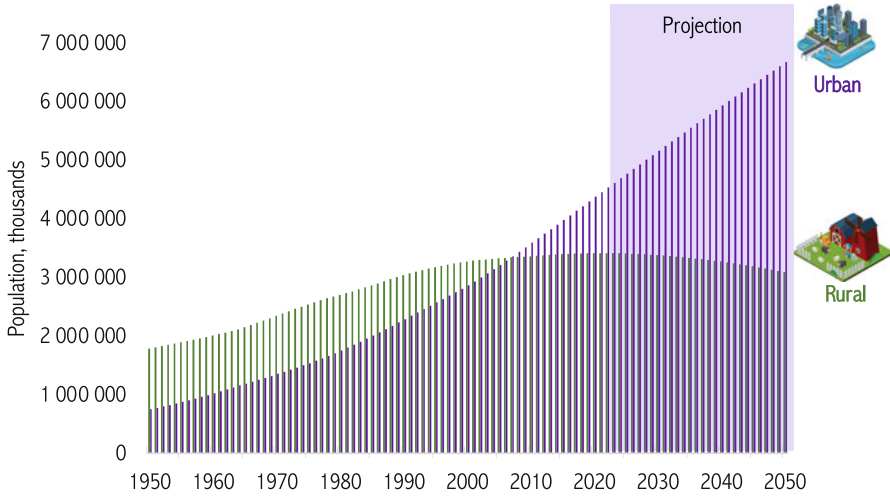


Fig. 1.1 Global urbanization, 1950–2050, thousands. Source: United Nation Department of Economic & Social Affair

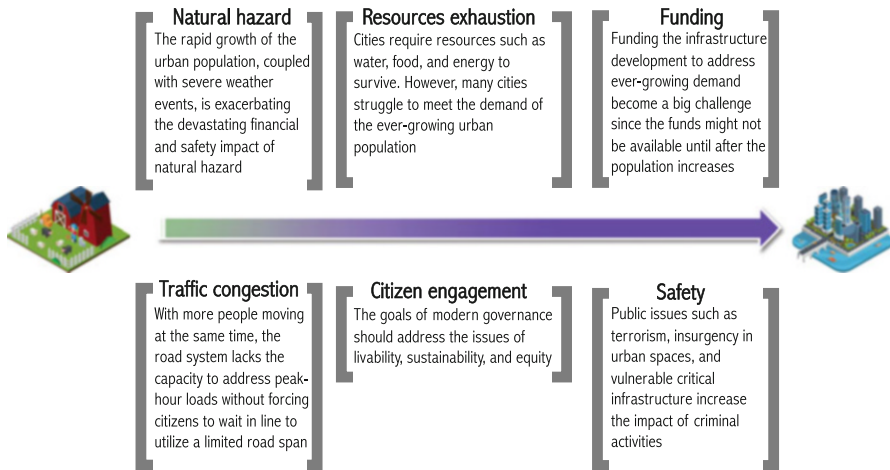


Fig. 1.2 Major challenges of modern cities

thirds of the world population will live in towns and cities by 2050 [19], implying that around 1.5 million people around the globe will move into urban areas every week [22].

This unprecedented population boom will put tremendous strain on urban infrastructure and comes with a myriad of challenges and opportunities. Natural hazards, resource exhaustion, sustainability of fiscal policies, traffic congestion, safety, and citizen engagement are only a few challenges modern cities face (Fig. 1.2.)