

**SECURITY RISKS OF URBAN
ELEMENTS
IN THE STREET ECOSYSTEM**

Meha Shukla

Supervisors: Dr. Shane Johnson, Peter Jones

Thesis submitted in partial fulfilment of the requirements for the degree of
Doctor of Philosophy, Security and Crime Science

**Department of Security and Crime Science
University College London (UCL)**

DATE: 19/12/2024

Student's Declaration

I, Meha Shukla, hereby declare that this thesis is my own original work. Where information has been derived from other sources, I confirm that this has been indicated in the thesis. I have clearly identified and acknowledged all source material used. No part of this thesis contains material previously submitted to the examiners of this or any other university, nor has any material previously been submitted for any other examination.

Meha Shukla

21 December 2024

Abstract

Streets are increasingly being redesigned with digital infrastructure, transforming traditional streets into connected places (formerly "smart cities"). However, there is limited understanding of the criminal risks these transformations may introduce. This research explores the criminogenic effects of both traditional and smart elements in urban street environments.

First, to establish a baseline, a systematic review of academic literature and meta-analyses was conducted to examine the effects of traditional urban elements on physical crime. The findings suggest that urban features, such as high pedestrian and traffic flow, shape crime opportunities, with busier places being more criminogenic.

Second, a review was conducted to explore the capabilities of digitally connected street infrastructure, the associated crimes, and security interventions. A systematic literature review of potential cyber-attacks on smart infrastructure in connected environments identified systemic risks (risk of a series of interconnected security events) and cascading failures (where a disruption in one infrastructure triggers a domino effect across interconnected and interdependent systems and services), posing a threat to essential national services.

Third, the challenges faced by UK local authorities in building cyber-resilience in connected places were explored, revealing that existing practices were inadequate for managing systemic risks and mitigating the cascading impacts of cyber-attacks.

The study highlights the need for a policy intervention and a national strategy to manage the systemic security risks of connected places. It also identifies the need for improved guidance, an assurance framework, and security governance to help local authorities procure, manage, and mitigate these risks.

While the findings have broader implications beyond the UK, they provide direct insights to the UK government, city authorities, and urban planners regarding gaps in integrating security and resilience into the design of evolving street ecosystems. Additionally, the study contributes to the academic literature on crime and place and offers insights for developing anticipatory policies.

Keywords: CPTED, Smart city, connected place, smart street, smart EV charging, smart city security, smart infrastructure security, smart city resilience, resilience, security by design, systemic risks, cyber risks, place managers

Impact Statement

This research tackles critical challenges related to the criminogenic effects of both traditional and digital urban elements, while also evaluating the effectiveness of security governance. It provides valuable insights for applying environment criminology theories to the security of connected places, an emerging area of research. The thesis offers crucial recommendations for Local Authorities (LAs) and Governments for integrating security and resilience into the planning and development of connected urban spaces, ensuring future cities are prepared for the complexities of a digital, interconnected world. It also offers policy improvements to safeguard connected built environments from emerging security risks. The key underlying themes of resilient design, risk assessment of holistic crime scenarios in smart environments, robust procurement processes for smart infrastructure, and governance of integrated smart systems can be applied to both current and future digital disruptions, including those expected from AI.

The findings of this research are both timely and highly relevant for interdisciplinary practitioners in urban planning, cybersecurity, resilience of connected places and the procurement of smart infrastructure. They offer practical guidance for anticipating criminogenic properties as emerging innovations, such as connected automated vehicles, are introduced in connected ecosystems. Additionally, the recommendations align with the UK's National Cyber Strategy 2022-2030, providing essential guidance for LAs, Government agencies, and policymakers in reducing the risks of cyber-attacks spreading across interconnected systems to Critical National Infrastructure (CNI) in connected places.

As part of the dissemination process, sections of this research have been published in an academic journal, as a deliverable for a European Union Horizon 2020 project, and in a policy paper released by UCL's Department of Science, Technology, Engineering, and Public Policy (STeAPP). The policy paper was reviewed by UK's Government Department of Science, Innovation and Technology (DSIT) and National Cyber Security Centre (NCSC), both of which expressed strong interest in exploring practical approaches for implementing the recommendations. The research on the "Security of Connected Places" was also presented at multiple international conferences.

The early findings from this study, including identified gaps in national guidelines for the cybersecurity of connected places, helped shape the scope of DSIT funded Alpha Testing project, where LAs were invited to test the guidance on cybersecurity for the rollout of smart infrastructure in Connected Places. DSIT also commissioned a review of global approaches and policies for the cybersecurity of connected places. The NCSC positively received the recommendations for enhancing cybersecurity guidelines for connected places. The Department of Transport and Connected Places Catapult acknowledged the finding that the smart streets manual lacked cyber resilience risk management and subsequently integrated common cybersecurity guidance for use cases. The study also influenced LAs, with one LA adding a requirement for a business continuity dry run in its procurement contract specifications based on the study's recommendations.

This research has the potential to have further impact, as it is aligned with UK Government's cyber security objectives and national cybersecurity strategy 2022-2030. It also has a broader impact beyond the UK, contributing to global efforts to enhance the cybersecurity of connected places.

Acknowledgements

I would like to express my gratitude to my supervisors at UCL, Dr. Shane Jonson and Peter Jones, for providing essential direction, research support, and ongoing encouragement throughout this thesis. I also thank Rob Guerette and Martin Andresen for their review and feedback on the systematic review protocol, and Michael Frith for his guidance on the meta-analysis.

I am grateful to all the stakeholders who participated in this research, were affiliated with it, and reviewed the findings. I acknowledge the ongoing engagement with the Chief Digital Officer (CDO) of London (Greater London Authority - GLA) and representatives from UK local authorities. Their support was crucial in completing this work.

The UK Government's Department of Science, Technology and Innovation (DSIT), the National Cyber Security Centre (NCSC) Connected Places team, NCSC Energy team, and the Department for Transport (DfT) provided invaluable direction and expert advice. Additionally, stakeholders such as the Energy Systems Catapult, Connected Places Catapult, Osprey (EV charge point operator), Tameside Metropolitan Borough i-Network, London Office of Technology and Innovation (LOTI), Local Government Association (LGA), and Syngenes Ltd. offered valuable insights into assessing cyber-resilience in connected places.

I would also like to thank Marco Franken (Product and Service Innovation Consultant) and Derek Tam (Technologist) for their ongoing support and regular discussions about my thesis. Finally, I would like to express my heartfelt gratitude to my family and friends for their personal support and interest in my research.

Abbreviations

List of frequently used Abbreviations

AI	Artificial Intelligence
ATM	Automated Teller Machine
CCTV	Closed Circuit Television
CNI	Critical National Infrastructure
CPNI	Center for Protection of National Infrastructure
CPO	Charge Point Operator
CPTED	Crime Prevention through Environmental Design
DCMS	Department for Culture, Media, and Sports
DOS	Denial of service
DDOS	Distributed Denial of Service
DfT	Department for Transport
DSIT	Department for Science, Innovation and Technology
EV	Electric vehicle
EVCS	Electric Vehicle Charging Station
EVSE	Electric Vehicle Supply Equipment
ICT	Information and Communications Technology
IoT	Internet of Things
IRR	Incident Rate Ratio
LA	Local Authority
NCSC	National Cyber Security Center
NIST	National Institute of Standards and Technology
NPSA	National Protective Security Authority
RAT	Routine Activity Theory
RCP	Rational Choice Perspective
SCP	Situational Crime Prevention
SR	Systematic Review

Contents

STUDENT'S DECLARATION	2
ABSTRACT	3
IMPACT STATEMENT.....	4
ACKNOWLEDGEMENTS	6
ABBREVIATIONS	7
1 INTRODUCTION	13
1.1 BACKGROUND – EVOLVING URBAN ENVIRONMENTS AND CRIME LANDSCAPE	13
1.1.1 <i>Traditional physical urban environments and crime</i>	14
1.1.2 <i>Crime and security in cyberspaces</i>	14
1.1.3 <i>Transforming urban environments</i>	17
1.1.4 <i>Changing crime risks in digitally connected places</i>	20
1.2 OBJECTIVES OF THIS THESIS.....	23
1.3 THE OUTLINE	24
1.4 DISSEMINATION	26
2 CRIME AND SECURITY IN URBAN PLACES	28
2.1 THEORIES OF ENVIRONMENTAL CRIMINOLOGY	28
2.2 PHYSICAL CRIME CONCENTRATION IN URBAN PLACES	35
2.3 ENVIRONMENTAL CRIMINOLOGY AND CYBER CRIME.....	41
2.4 ENVIRONMENTAL CRIMINOLOGY - CRIMES IN CONNECTED PLACES.....	46
2.5 SUMMARY	49
3 STUDY OF PHYSICAL CRIME PATTERNS WITHIN THE BUILT ENVIRONMENT	52
3.1 STUDY DESIGN.....	53
3.1.1 <i>Search Strategy</i>	53
3.1.2 <i>Criteria for inclusion and exclusion</i>	57
3.1.3 <i>Approach to Meta-analysis</i>	59
3.1.4 <i>Grouping data for meta-analysis</i>	60
3.1.5 <i>Methodology for meta-analysis</i>	60
3.2 SEARCH RESULTS.....	63
3.2.1 <i>Screening of search results</i>	63
3.2.2 <i>Data Extraction</i>	65
3.2.3 <i>Characteristics of included studies</i>	65
3.3 META-ANALYSIS.....	68
3.3.1 <i>Street Network, Configuration and other features</i>	69
3.3.2 <i>Public Transit</i>	77
3.3.3 <i>Parks</i>	82

3.3.4 Schools	87
3.3.5 Alcohol outlets	91
3.3.6 Retail land use.....	96
3.3.7 Drug treatment centers	101
3.3.8 Bank Branches and ATMs	102
3.3.9 Other urban elements	103
3.4 DISCUSSION	105
4 URBAN SMART INFRASTRUCTURE AND SECURITY CHALLENGES	112
4.1 BACKGROUND – DIGITAL TRANSFORMATION OF THE URBAN STREET ELEMENTS	114
4.1.1 Basic elements of Digital Transformations	114
4.1.2 General implications of digital transformations on crime and security	120
4.2 DIGITAL CAPABILITIES AND CYBER RISKS OF SMART INFRASTRUCTURE.....	126
4.2.1 Sampling of smart infrastructure use cases	126
4.2.2 Smart CCTV	128
4.2.3 Smart Lighting columns	134
4.2.4 Smart EV charging	138
4.2.5 Smart Bus stops.....	143
4.3 CASCADING IMPACTS OF CYBER-ATTACKS IN CONNECTED PLACES	147
4.3.1 Focus of the systematic literature review	149
4.3.2 Search strategy	150
4.3.3 Criteria for screening of search Results	151
4.3.4 Data extraction	151
4.4 RESULTS – SYSTEMATIC LITERATURE REVIEW	153
4.4.1 Summary of search results.....	153
4.4.2 Smart CCTV	155
4.4.3 Smart Lighting columns	157
4.4.4 Smart EV charging	158
4.5 DISCUSSION.....	167
4.6 CONCLUSION	174
5 ASSESSMENT OF CURRENT SECURITY MEASURES IN CONNECTED PLACES	176
5.1 AIM, RESEARCH QUESTIONS, AND APPROACH.....	177
5.2 STUDY DESIGN.....	178
5.2.1 Methodology.....	178
5.2.2 Stage 1-Preparation.....	179
5.2.3 Stage 2-Data gathering.....	186
5.2.4 Stage 3- Further analysis.....	193
5.3 RESULTS FROM STAGE 2 (DATA GATHERING).....	193

5.3.1 Results – Stage2 - Phase1	194
5.3.2 Results – Stage2 - Phase 2: General questions.....	197
5.3.3 Results – Stage 2 - Phase 2: Conformance to cybersecurity principles	201
5.3.4 Summary of Results - Discussion	219
5.4 RESULTS FROM STAGE 3 (FURTHER ANALYSIS)	223
5.4.1 Critical assessment of NCSC guidance.....	223
5.4.2 Thematic analysis of gaps in the procurement process	225
5.4.3 Root-Cause Analysis.....	226
5.5 DISCUSSION	231
5.5.1 Capabilities for management of systemic cyber risks in the ecosystem	233
5.5.2 Management of cyber resilience in the procurement process of smart services	237
5.6 CONCLUSION.....	241
6. SUMMARY AND IMPACT OF THIS RESEARCH	243
6.1 RESEARCH STAGES AND FINDINGS	243
6.1.1 Stage 1: Criminogenic effects of urban elements of street environment.....	243
6.1.2 Stage 2: Digital capabilities and cybercrime risks of smart infrastructure	245
6.1.3 Stage 3: Cybersecurity risks of connected places.....	246
6.2 RECOMMENDATIONS	249
6.3 LIMITATIONS OF THIS RESEARCH	252
6.4 RECOMMENDED FUTURE RESEARCH	254
6.5 IMPACT OF THIS DOCTORAL RESEARCH	255
REFERENCES.....	258
APPENDIX 1	313
APPENDIX 2	320
APPENDIX 3	322
APPENDIX 4	342
APPENDIX 5	345

List of Tables

Table 3.1 Urban Elements found in studies included in SR.....	66
Table 3.2 Statistical models used by studies in SR	67
Table 3.3 Influence of Street Configuration on crime - Assessment of studies for inclusion in meta-analysis	70
Table 3.4 Data Analysis-Influence of Street Configuration on crime grouped by predictor variable and crime type.....	74
Table 3.5 Influence of Public Transit on crime -- Assessment of studies for inclusion in meta-analysis	79
Table 3.6 Data Analysis-Influence of Public Transit on crime grouped by predictor variable and crime type.....	81
Table 3.7 Influence of Parks on crime – Analysis of studies for inclusion in meta-analysis	84
Table 3.8 Data Analysis-Influence of Parks on crime grouped by predictor	85
Table 3.9 Influence of Schools on crime –Analysis of studies for inclusion in meta-analysis	88
Table 3.10 Data Analysis-Influence of schools on crime grouped by predictor variable and crime type	89
Table 3.11 Influence of Alcohol outlets on crime – Analysis of studies for inclusion in meta-analysis.	92
Table 3.12 Data Analysis-Influence of Alcohol outlets on crime grouped by predictor variable and crime type.....	94
Table 3.13 Influence of Retail land use on crime – Analysis of studies for inclusion in meta-analysis	97
Table 3.14 Predictor Variables-Influence of Retail land use on crime	100
Table 3.15 Other urban elements and association with crime	104
Table 4.1 Sample applications of sensors on streets	116
Table 4.2 Government interventions for cyber-security risks of connected places and smart infrastructure services	125
Table 4.3 Selection of use cases	128
Table 4.4 Search Keywords for literature review	150
Table 4.5 Hierarchy of evidence – systematic review of cascading impacts of a cyber-attack.....	153
Table 4.6 Number of cascading impacts found in studies included in systematic literature review ...	155
Table 4.7 Studies for smart streetlight included in systematic literature review to study cascading impacts of cyber-attacks	155
Table 4.8 Studies for smart streetlight included in systematic literature review to study cascading impacts of cyber-attacks	157
Table 4.9 Studies for smart EV charging included in systematic literature review to study cascading impacts of cyber-attacks	159
Table 4.10 Hierarchy of evidence found in systematic review of cascading impacts of cyber-attacks on smart infrastructure.	161
Table 5.1 Selection of NCSC cybersecurity principles for connected places	181
Table 5.2 Stakeholders identified from the UK Government (Group 1)	183
Table 5.3 Stakeholders associated with the UK's LAs (Group 2)	186

Table 5.4 Stakeholders in Data gathering Phase 2 to study procurement of smart services	189
Table 5.5 Stakeholders identified for the focus group (Group 3)	189
Table 5.6 Research Participants and Questionnaire for second phase of data gathering	191
Table 5.7 Non-conformances: Local authority' procurement process and the NCSC cybersecurity principles for connected places.....	221

List of Figures

Figure 1-1 Research Design	24
Figure 2-1 Crime Triangle	29
Figure 2-2 Hierarchy of spatial units	39
Figure 3-1 Prisma Chart of search process for systematic review	64
Figure 3-2 Forest plot – Influence of Street Configuration on crime	76
Figure 3-3 Forest plot – Influence of Public Transit on crime	82
Figure 3-4 Forest plot for Influence of Parks on crimes	86
Figure 3-5 Forest plot for Influence of schools on crimes	90
Figure 3-6 Forest plot for Influence of Alcohol outlets on crimes	95
Figure 3-7 Forest plot for Influence of Retail land use on crimes	101
Figure 3-8 Forest plot for Influence of Drug treatment centres on crimes	102
Figure 3-9 Forest plot for Influence of Bank branches and ATMs on crimes	103
Figure 3-10 Forest plot – summary of the estimated Influence of Urban elements on crime	106
Figure 4-1 Smart CCTV system	130
Figure 4-2 Connected place lighting columns.....	135
Figure 4-3 EV charging points.....	139
Figure 4-4 Smart EV charging	140
Figure 4-5 Smart bus stops and shelters	144
Figure 4-6 Prisma chart.....	154
Figure 4-7 Smart EV charging cascading impacts - One incident at massive scale	162
Figure 4-8 Smart EV charging cascading impacts - Multiple incidents at massive scale	164
Figure 5-1 Overview of Study Design	178
Figure 5-2 Stage-1 of the study – Preparation.....	179
Figure 5-3 Stage-2 of the study – Data Gathering.....	187
Figure 5-4 Stage-3 of the study – Further Analysis	193
Figure 5-5 Theme 1 - Root cause Analysis.....	227
Figure 5-6 Theme 2 - Root cause Analysis.....	228
Figure 5-7 Theme 3 - Root cause Analysis.....	229
Figure 5-8 Theme 4 - Root cause Analysis.....	230
Figure 5-9 Theme 5 - Root cause Analysis.....	231

Chapter One

1 Introduction

This doctoral thesis identifies and assesses the criminogenic aspects of urban elements in the street ecosystem. The purpose is to explore the (changing) nature of urban streets, analyse the potential implications for crime, explore available security interventions and provide guidance for urban designers and other city authorities to encourage them to think about security and crime prevention. A street ecosystem refers to the dynamic interactions between various urban elements (such as roads, parks, buildings, and schools) and people in an urban built environment. The research presented assesses both traditional physical and digitally enabled urban elements for their influence on security risks in the street environment. This chapter initially provides a background to the criminogenic features of the physical built environment, cyberspaces, the digital transformation of urban elements and their potential influence on crime. It is not intended to be exhaustive as the purpose is to introduce the topic and the focus of the chapters that follow. The remainder of this chapter discusses the research aims, approach taken, and provides an outline of the thesis.

1.1 Background – evolving urban environments and crime landscape

Urban environments and their design have to cater for the changing needs of travel, and places for social interactions by creating a balance between movement and place functions (DfT, 2007). Urban elements in built environments now encompass both traditional physical components and digitally connected elements, where human activities influence the functionality and experience of urban spaces. The continuously changing built environment, our extensive use of the internet, the changing nature of public services, shifts in movement patterns, new business models, and peoples' evolving interactions with places have affected the crime and security landscape (Europol, 2015). City authorities and urban planners adapt to these changes with the aim of creating built environments that improve the quality of people's lives.

1.1.1 Traditional physical urban environments and crime

The traditional physical built environment can be defined in a number of ways but essentially encompasses not just the availability but also the quality of neighbourhoods, buildings, urban spaces, walkways, roads, parks and all the other “human-made” surroundings (Hassen & Kaufman, 2016; Renalds et al., 2010; Roof & Oleru, 2008). Research in the field of environmental criminology (further explained in Chapter 2) has studied how elements of traditional urban environments such as street length, public facilities, street furniture and residential housing influence the spatial and temporal distribution of crime (Beavon et al., 1994; Brantingham & Brantingham, 1995; Eck, Clarke, Guerette, et al., 2007; Frith et al., 2017; Hart & Miethe, 2015; Kim et al., 2017; Weisburd et al., 2016a). Using more complete knowledge of what generates crime hot spots in space and time, designers can reduce criminal opportunity by designing places that reduce the risk of crime. For example, permeable street layouts have been shown to increase crime levels (Armitage, 2013), while installing street lights on dark streets has been shown to reduce crime (Xu et al., 2018). Therefore, an understanding of the distribution of opportunities, crime patterns, security interventions and any potentially harmful effects of interventions can inform decision making concerned with the specific security aspects of urban design and crime-control policies (Barr & Pease, 1990; Rondeau et al., 2005; Welsh et al., 2014).

1.1.2 Crime and security in cyberspaces

It was estimated that 5 billion people (more than half of world’s population) use the internet in 2024 (Forbes Home, 2024). Since the advent of the internet, innovation and technological advances, peoples’ activities in cyberspaces and changing behaviours have led to the evolution of cybercrime and the cybersecurity landscape. According to Miró-Llinares and Johnson (2018), cyber places constitute different activity spaces just as geographic places do. For example, sites for entertainment, leisure, games, shopping, workplace meetings and socialising all encourage or facilitate different types of activities (Miró Llinares & Johnson, 2018a). Because of the ease of remote interactions, advancements in technologies, and a lack of uniform law enforcement for online crime across countries, criminal opportunities multiply which can result in new cybercrimes, shifts in targets, new methods of committing cybercrimes, shifts in victims targeted and changes to the way offenders operate (Leukfeldt et al., 2020). Advances in technology and vulnerabilities in networks and

software have facilitated a sophisticated global online business. Reacting to these opportunities, cybercriminals began to operate professional ventures such as the creation of botnets (i.e. thousands of infected computers owned and controlled by the cybercriminal) and take advantage of the dark web¹ (a collection of hidden internet sites not created by but most commonly used by criminals), where transactions of stolen goods and illegal services are conducted professionally (Mirea et al., 2019). The formation of a criminal supply-chain gave rise to cybercrime-as-a-service where complex criminal activities (such as the spreading of malware, the sale of illicit drugs, and conducting ransomware attacks) are outsourced to professionals often through the dark web (Huang et al., 2017). This also helped cybercrime increase in scale at a much faster rate.

The vulnerabilities in developing technologies, networks, business processes and human awareness have resulted in wide-spread cyber-enabled (Increase in scale or reach of traditional crimes using Information and Communications Technology - ICT), cyber-dependent (crimes that cannot be committed without using ICT), cyber-assisted (Crimes that are assisted by cyber means) and cyber-physical crimes (attacks on physical infrastructure and essential services through cyber means) (Shelden, 2018; Tzezana, 2016). Ransomware attacks are one form of crime that has been facilitated by the (pseudo)anonymity and cross-border transfers of value that technology such as the block chain (Remrey & Maimon, 2016) and cryptocurrencies provide to offenders (Escalante & Capstone, 2018). Examples of other cybercrimes committed against individuals, organizations and society include cyber stalking (Vakhitova et al., 2016), identity theft (Blythe & Johnson, 2021), financial loss due to fraud in mobile banking services (Maulana et al., 2019), online copyright infringement (Clough, 2015), obtaining sensitive data such as intellectual property or trade secrets by hacking into data systems (Rege, 2014), and spreading radicalising propaganda online (Mughal et al., 2023). Social media platforms (where presence of real people and organizations is now vital) are also unintentionally criminogenic in nature. People share personal as well as professional information on social media that can be vulnerable in general, and vulnerable to potential data breaches in particular (Yar, 2012; Rajesh & Ramesh, 2016). Social media is now used on a much larger scale by

¹ Ian Clarke from University of Edinburgh in 2020 launched Freenet, a program that allowed the use of internet without disclosing the identity of the user; the origin of dark web used for illegal cyber activities can be traced to Freenet (Goode & Goode, 2011; Orabi, 2024).

organized criminals to manipulate public opinion, influence democratic election outcomes, spread fake news and disinformation, and cause harm to individuals and society (Raman et al., 2020; Vaccari & Chadwick, 2020). For example, in 2011, London, United Kingdom (UK) witnessed the collaborative use of social media platforms to organise and respond to disorder on streets (Williams et al., 2013).

The years 2016 and 2017 were a global wake-up call about the unprecedented nature of the developing cyber-warfare threat landscape and how this could impact upon national essential services. The UK experienced the Wanna cry ransomware attack in 2017 which left many National Health trusts crippled (Black, 2018). In 2016, an attack on Critical National Infrastructure (CNI) occurred in the Ukraine when a power grid was attacked by hackers allegedly backed by the Russian government clearly demonstrating the risks of cyber-attacks on essential services by hostile nations (Niranjan, 2022). Regulatory control through risk management capabilities has been introduced by many countries to protect against cyber-physical attacks on CNI (Dimase et al., 2015). However, the concept of cyber-physical system security is not consistently defined and requires an integrated approach across various domains such as physical, information, cognitive, social, business processes, technology, safety and risk management (Dimase et al., 2015).

Speedy interactions in the virtual world, such as real-time transactions and information sharing on social media, accelerate the rate at which offences can be committed. Since offenders can commit crimes remotely in cyberspace and can move quickly across a wide range of digital platforms, patterns of cybercrime can differ from traditional crimes in physical environments (for which offenders are subject to physical constraints). Insufficient regulations and inadequate laws in some countries make it difficult to prevent cybercrime. Due to the global nature of the internet and the absence of a central authority, the legality of activities in digital spaces also differ by the country where the crime originates and countries where other people are involved as well as impacted. However, geography does play an indirect role, as offenders may be constrained in reaching suitable targets from countries that have stronger regulatory environments or efficient law enforcement practices in digital spaces (Llinares, & Johnson, 2018). Law enforcement is constrained in combating cybercrime as investigations tend to cross overlapping jurisdictions and require a large amount of coordination (Phillips, 2017).

Cyber-security has evolved from security measures for individual computers, network security, international treaties, to national level security strategies with international collaboration. Policy, regulations and international treaties such as the Budapest Convention (Hinduja & Kooi, 2013) have been used as a tool to counter data breaches, information theft, privacy violation, denial of service and manipulation attacks (Covington & Carskadden, 2013; Khey & Sainato, 2013). Most security policies and procedures that safeguard the confidentiality, integrity and availability of data were initially technologically inclined (Samuels, 2005). Security has evolved further wherein Governments have introduced legislations and standards to address cyber-crime. Examples include the UK Data protection Act 2018 (DPA), the European Union (EU) Cybersecurity Act 2019, the EU Global Data Protection Regulation-2018 (GDPR), the UK Government's Online Safety Act (OSA) and the global ISO 27001 standards for information security (Legislation.gov.uk, 2023). The UK National Security Act 2023, updated existing laws to ensure that unauthorised access of a prohibited place applies not just to access by physical means but also by electronic/remote methods (House of Commons, 2023). Due to the rapid pace of technological change and evolving cybercrime tactics, most organizations require time to transition from outdated security practices to those that address current cybercrime risks. Given the latency associated with doing so, many organisations find themselves subject to cyber-attacks.

1.1.3 Transforming urban environments

In 2015, countries worldwide, including the UK, recognized that infrastructure, resources, and urban services were stretched and unsustainable (Khatoun & Zeadally, 2017; Webb et al., 2018) because by 2050, population growth is expected to rise by 16% in urban cities (ACN Newswire, 2015). The number of cars and light trucks on urban roads are expected to rise by almost three times as many as there were in 2015 ("Streetwise; Urban Planning," 2015). In response, worldwide city planners (and others) are redefining and redesigning streets – streets that are currently dominated by vehicular movement – to provide places that facilitate public interaction, enable greater accessibility and reduce congestion (ACN Newswire, 2015; Adams, 2016; Ambrosino et al., 2016). This is intended to lead to changes in built environments for sustainable development that encourage walking, a shift from cars to cycling, flexible mobility solutions, the dynamic allocation of road space, multi-modal shared

connected transport, and data driven efficient urban services (Garcia-Font et al., 2016; W. Li et al., 2018; Marcucci et al., 2017; McGrath, 2004; Ogilvie et al., 2004; Prasad, 2009; Yang et al., 2010).

Sustainable development initiatives are driving the evolution of urban spaces using applications of the “smart city” urban development concept (Andrade et al., 2021). A community that uses technology, and gathers data to monitor the real world in real time and uses information to improve services and the quality of life for its citizens was initially known as a smart city (Mijac et al., 2017; Lacinák & Ristvej, 2017). Smart streets are a key element of smart city concepts, serving as the “basic building block for any smart city architecture”. (Pribyl & Pribyl, 2015). In the UK, the National Cyber Security Centre (NCSC), now refers to smart cities and smart street ecosystems as connected places (NCSC, 2021a).

With the advent of Industry 4.0 (the digital technology revolution) there has been a continuous transformation of urban elements (Oztemel & Gursev, 2020). Innovation and digital transformation is increasingly connecting elements of urban infrastructure and devices used by people to enhance urban services by bringing together different technological advances such as telecommunications (3G,4G,5G), the Internet of Things - IoT (i.e. internet connected devices/infrastructure), OT (Operational Technology – used for critical infrastructure and industrial environments) and Industrial Internet of Things (IIoT) (i.e. IoT used for industrial applications), (Heidari et al., 2023; Toh et al., 2020a; Vermesan et al., 2020). Artificial Intelligence (AI) (a technology intended to enable computers to mimic human intelligence) and machine learning enable intelligent data processing, the recognition of patterns, automation, and informed predictions (Heidari et al., 2023; Vermesan et al., 2020). Additionally, the use of digital twins using Augmented Reality (AR) and Virtual Reality (VR) technology enables the use of digital replicas of physical objects (such as urban elements on streets) to simulate functions using real-time data, to gain insights into the effectiveness of proposed smart solutions (Salvi et al., 2022; Vermesan et al., 2020).

Smart initiatives in urban cities have resulted in cyberspaces now being connected to real places in many ways that alter the experience of people and communities. For example, the advent of 5G technology allows real-time data sharing between vehicles, street infrastructure, and IoT devices used in smart urban environments over wireless networks for potentially efficient journeys. This has

allowed city authorities to conduct tests of self-driving vehicles in cities across the world including the first full-sized self-driving bus in the UK (GOV.UK, 2023b). Access to new/ enhanced electronic devices, on-line applications and smart IoT-based infrastructure services have become important in the day-to-day activities of people, organizations and society worldwide. Smart initiatives in urban cities aim to provide integrated services using a connected five layered collaborative operating model (*BSI Standards Publication PAS 181:2014*, 2014; Prislán & Slak, 2018):

1. Technology and Infrastructure – This layer includes sensors, networks, actuators, hardware data centres and software. A sensor is a device that detects inputs from a physical environment. For example, a streetlight sensor can detect and collect data on levels of illumination. In turn, an actuator can act on this data to change the brightness level of the streetlights in the network, with this action being determined by the chosen settings of the streetlight administrator.
2. Data – This layer includes real-time open city data and is managed as an asset e.g., the reading of the licence plate of a car in real-time.
3. Integrated city-wide governance – This layer includes transparent and open data insights aimed at effective operations and the governance of city services.
4. Services – This layer includes co-created (public/private/social-enterprise/citizen) shared services intended to ensure the real-time integration and optimization of city resources using city data. E.g., smart parking, gunshot detection.
5. Customer delivery – This layer is about delivering user-centric services to customer groups such as pedestrians, elderly people, drivers, cyclists, and commuters for example, through mobile software applications.

The digital transformations taking place in the 21st century are being enabled by data collection and communication between users, sensors, devices, and urban cyber-physical street infrastructure (Park, 2022). Connected place projects aim to transform existing streets through networked sensors that gather data about traffic, pedestrians and the environment within which the street operates with the aim of providing efficient services and using the urban spaces effectively (Pribyl & Pribyl, 2015). This has resulted in changes to urban elements in the street ecosystems to include: a) smart places with new elements (such as digital kiosks, footway robots, e-

scooters), b) changes in the way existing elements in the built environment look or operate (such as socially distanced benches with charging options, payments for parking meters through mobile apps, innovative solutions for speed reduction such as 3D zebra crossings (Euro Cities, 2021)), c) an increase in the number of specific elements on streets (for example, the video surveillance market in the UK is expected to grow annually by 4.9% between 2022 and 2027: Markets and Markets, 2022), d) enhancements to the functionality of street elements (such as live schedule displays at bus stops) and e) some street elements being phased out or repurposed (e.g. phone booths, post boxes) (CBS News, 2016; Kollwe, 2021; MORE, 2022c).

AI and technology based retail transformations lead to increase in the number of channels in the business process during the Covid-19 pandemic (Priporas et al., 2017; Mahmoud et al., 2020; Abbu et al., 2021). Examples include usage of lockers for deliveries to facilitate on-line shopping and virtual fitting rooms (that allow people to see how clothes look and fit on a person's body using mobile applications) (Priporas et al., 2017; Mahmoud et al., 2020; Abbu et al., 2021). This has also contributed to changes in patterns of movement and crime.

City authorities, planners and urban designers are focusing on transformational change through public-private collaboration to resolve the challenge of providing scalable, cost-effective and efficient solutions and ultimately a good quality of life (Mijac et al., 2017).

1.1.4 Changing crime risks in digitally connected places

In some urban areas there are connected places where roads, sidewalks, parks, buildings, vehicles, lamp posts, traffic lights and other street furniture are already digitally connected using IoT devices and information such as pedestrian flow, parking spaces and building occupancy is collected, shared and communicated to facilitate efficient integrated services (Galle et al., 2019; Prislán & Slak, 2018; Truntsevsky et al., 2018). While this is clearly beneficial, where it is not managed properly, it will have increased the attack surface and cyber threats further, and hence more and more diverse attacks are expected in the future (Hammi et al., 2018). In 2015, Europol predicted that such changes will lead to emerging threats that do not have a historical precedence (Europol, 2015). For example, 3-D printers are now used to reproduce physical objects from digital files in many industries such as weapons manufacturing, aerospace, medicine, engineering and construction, education, and retail which poses

various challenges such as copyright and intellectual property violations (Fang & Kumar, 2019). It also enables the do-it-yourself printing of guns that can be used by criminals (Jacobs & Haberman, 2017; Oztemel & Gursev, 2020). Offenders have also shifted their targets to attack vulnerable elderly people with less knowledge of digital applications (Strupczewski, 2024) and charity business structures that had comparatively lower security levels (Riadi et al., 2022). Another shift in targets has resulted from the IoT connecting objects such as streetlights, coffee machines, smart cars, buildings, energy meters, roads, parking metres, smart phones and pacemakers over the internet. While this connectivity improves their functionality, digitally connected infrastructure has provided hackers with more available targets in the form of “things” such as Closed-Circuit Television (CCTV), smart TVs and electric smart meters, which creates the opportunity to disrupt the day-to-day life of people, potentially at scale. IoT-based infrastructure and devices expose consumers to victimization risks and manufacturers need to build in more security to protect against cyber-criminal misuse (Blythe et al., 2020).

New innovative products and services supported by technological innovations could lead to crime harvests unless scanning is undertaken to identify new threats, to assess new criminal opportunities, and to embed security upfront (Armitage & Pease, 2008; Ekblom & Pease, 2014). For example, criminal opportunities were overlooked when the internet, credit cards and mobile phones were first introduced (Armitage & Pease, 2008; Guerette & Clarke, 2003; Mitchell, 2012; Monahan, 2009). While this was not the case initially, smart product manufacturers and smart infrastructure designers are now made liable by Governments to build in security-by-design and adopt common standards to prevent cyber-attacks (Blythe et al., 2020). For example, the US Government implemented ‘The Internet of Things (IoT) Cybersecurity Improvement Act of 2020’, which provides a framework and guidelines for cybersecurity risk management for the agencies that manage IoT devices. (Gianluca, 2016; US-Congress.Gov, 2019). However, there is not enough evidence on whether these measures are effective.

Security mechanisms are also changing in response to crimes made possible by evolving technologies in connected places. Data aggregated from sensors enables real-time monitoring applications, 24/7 Video Analytics and integrated services through smartphone and other user interfaces (e.g. web portals). Examples include abuse detection for a smart lighting network (Andrysiak et al., 2017), detecting

intrusion using thermal imaging (Pawłowski et al., 2020), the automated reading of vehicle licence plates to detect violations (Pawłowski et al., 2020), and the detection of pedestrian behaviour from wearable sensors (Hundal et al., 2020). Guidelines have been published for the cyber security of innovations such as smart automated cars (HM Government, 2017) and new products such as drones (ICO, n.d.). New analytic, surveillance, and detection technologies are being developed to combat cybercrime, e.g., a drone detection system can identify hostile drones (Heidari et al., 2023). Data analytics across the urban environment, and technologies such as AI, can provide new, possibly real-time inputs to the development of crime prediction models (Lee et al., 2019). However, the evidence base is limited regarding whether security interventions, as well as the governance provided for smart initiatives, delivers what is required for secure urban cross-sector services (Shukla, 2021; Shukla et al., 2019).

The digital infrastructure builds cyber-physical environments that connect a single environmental unit to multiple components of a city, thus, providing a path to attack CNI connected to smart infrastructure (such as smart Electric vehicles) in built environments (Joo et al., 2018; Laufs, Borrión, & Bradford, 2020). These cyber-attacks on smart street infrastructure could potentially result in cascading impacts wherein the disruption of one system could lead to a “domino effect” across inter-related and inter-connected digital systems in connected places. This could lead to catastrophic impacts on essential CNI services. Consequently, it is also important that mitigations are implemented at the design stage of the transformation of urban street environments to ensure that cascading impacts, should they occur, are contained and that harmful effects to essential national public services are minimised (NCSC, 2021a; NCSC, 2022b). Design against crime (and secure by design) is a proactive approach to crime reduction that involves anticipating threats and then attempting to design potential interventions before products and services are rolled out. This contrasts to other approaches that involve retrofitting solutions reactively to minimize the impact of crime harvests after they start to emerge (Blythe & Johnson, 2021; Ekblom & Pease, 2014; Farrell & Pease, 2006; Kinney et al., 1978). Security-by-design is required for innovative IoT devices ranging from smart devices in homes to industrial control systems to prevent an IoT crime harvest (Blythe & Johnson, 2021).

Designing and implementing security has now become a very complex process given the potential for fast-paced dynamically changing criminal landscapes (*Europol*, 2015). Designers and manufacturers are responsible for security-by-design of their

products and services (Ekblom & Pease, 2014). Research findings indicate that urban planners also recognise the importance of security-by-design, however it is often overlooked as it is a low priority compared to other planning criteria leaving vulnerabilities in products and services (Armitage & Pease, 2008; Bowers, 2014; Knapp, 2013). Legislative, regulatory, security-by-design, and anticipated policy frameworks are challenged by the changing crime landscape, coupled with fast-paced technological developments adapted by society (Shukla et al., 2019). The accountabilities for smart urban design, planning, approval processes and assessment of the crime risks in transforming built environments are distributed (Clancey et al., 2018; Monchuk, Anderson, & Ellis, 2018). There is therefore a need to understand the collaborative management of smart security risks and governance across urban planning, transportation, law enforcement, and public administration (Colenbrander & Barau, 2019).

1.2 Objectives of this thesis

This thesis attempts to answer the research question “How might changes to urban elements in the street environment affect physical and cybercrime risks?” The aim of this research is to assess the potential criminogenic features and criminal misuse presented by traditional physical and digitally enabled urban elements on streets to inform “anticipatory” policy that might address them. The study intends to help urban designers, local authorities, policy makers, businesses, citizens, city officials and regulators across sectors to a) understand the potential crime risks in the built ecosystem caused by the changing design of urban elements in the built environment and b) incorporate security-by-design at the outset rather than at a later stage when it becomes difficult or impossible to retrofit.

To meet the aims of the research it is important to define the urban elements that are in scope for the research reported. This thesis focuses on the public street environment. The scope of work focuses on the influence of the outdoor physical elements of urban streets (places such as carriage way, footway, parks) on crime occurrence. Although buildings are considered in scope, the focus will be on the influence of features of the building on street environment (e.g., criminogenic properties of schools and bars in the built environment). The sub surface (e.g., under the ground utility pipelines) are not in scope, however, the influence of underground public transit of on crime are in scope. The internal aspects of the urban elements (e.g.

internal features of a building or subway station) are not in scope. The methodological approach for this study was divided into five stages (see Figure 1-1).

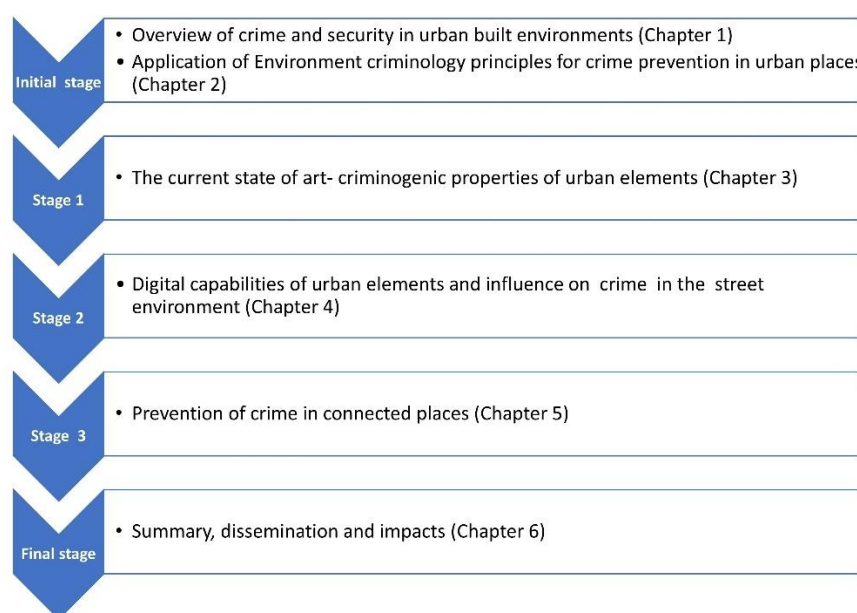


Figure 1-1 Research Design

In the initial stage, an overview of crime and security in urban places (Chapter 1) and the principles of crime prevention through environmental design (Chapter 2) are explained. Stage 1 aimed to take stock of existing research to establish how elements of the built environment have been found to affect crime in previous work (Chapter 3). Stage 2 aimed to explore the available research specific to cyber-threat scenarios for smart street infrastructure systems, which could potentially spread across the networks in connected places, causing disruption to CNI (Chapter 4). The aim of stage 3 was to provide evidence-based empirical analysis of the challenges faced by the UK's Local Authorities (LAs) in building Security-by-design within the smart infrastructure procurement processes to protect the CNI from the impacts of cyber-attacks on connected systems (Chapter 5). Finally, all the stages of research are brought together and summarised (Chapter 6). The description of each stage and chapter in this thesis is described in detail next.

1.3 The Outline

This thesis is organised into six chapters. **Chapter 1** introduced the research topic, the purpose of the research, and provides an overview of the approach, outline of the thesis and the dissemination of the research. **Chapter 2** introduces theories of

environmental criminology that have informed urban design decisions and provides a narrative literature review of how they are applied to physical, cyber and smart initiatives in connected places. This chapter provides the groundwork for the research described in stages 1,2, and 3.

Chapter 3 (Stage 1) explores the academic literature to understand how various urban elements such as the configuration of the street network, parks, and schools have been found to influence crime. The existing literature on the criminogenic properties of the built environment and the mechanism(s) through which land use might generate different types of crimes are examined through a systematic review. The review takes stock of the literature to understand the criminogenic properties of urban elements within the street ecosystem (e.g. bus stops, alcohol outlets and parks) on crime. The review also analyses how researchers have estimated the impact of cyber activities in the street ecosystem. A qualitative synthesis of all identified studies was initially presented. A statistical meta-analysis was then presented for those studies for which sufficient data were available. The meta-analysis provided a baseline of the quantified criminogenic effect of street elements currently found in urban environments, the purpose of which was to anticipate the impact of changes. As a standalone exploratory study, it contributes to academic literature to present the state of the art regarding the effects of traditional physical urban elements on crime prior to researching the digital urban elements that now co-exist with the physical elements.

Chapter 4 (Stage 2) focuses on the digital urban transformations that may create new crime opportunities. CNI is an attractive target for cyber-attacks in connected places (Yunos & Hafidz Suid, 2010), and hence, recommendations from this research prioritizes the reduction of impacts to CNI. The research is divided into two phases – 1) The study of urban street transformations and the criminogenic risks of smart infrastructure in the street ecosystem; and 2) The study of potential cascading impacts of cyber-attacks on smart infrastructure to the CNI in connected places. The objective of the first phase was to explore the transformation of current urban streets to smart streets and the resulting changes to crime and security in connected places that these might produce. A narrative review was conducted on the digital capabilities of the smart infrastructure of streets, changes to people's behaviors and how these changes may potentially influence crime. In-depth case studies are presented, and these consider CCTV, Street lights, Electric Vehicle (EV) charging and bus stops. The

cybercrimes associated with these use cases and their impact on connected services are outlined.

The second phase explored the literature to understand the extent of available research on how a cyber-attack on one element of smart street infrastructure could cause cascading impacts to inter-related / inter-connected systems. The aim was to assess the potential disruption of CNI in a connected place which could potentially lead to a catastrophic impact to essential national services. A systematic literature review was conducted to synthesise knowledge on cascading impacts of cyber-attacks on smart infrastructure.

Chapter 5 (Stage 3) complements the findings from Chapter 4 with an evidence-based analysis of how a sample of LAs manage the cybersecurity risks of smart street infrastructure to prevent cascading impacts to CNI in connected places. LAs procure and rollout smart services in partnership with private service operators and hence a study was conducted to assess whether the security capabilities embedded in the procurement process of smart services by the LAs were fit for purpose, and secure by design. Interviews were conducted with relevant stakeholders to gather qualitative data and explore the challenges associated with embedding cyber-resilience by design. Potential crime scenarios for the changing smart street elements from Chapter 4 were analyzed against the guidelines for the cybersecurity of connected places provided by the NCSC, the UK's technical authority that provides guidance and advice on cybersecurity (NCSC, 2022c). A thematic gap analysis was conducted followed by an analysis to understand the root causes for the occurrence of gaps. The chapter concludes with recommendations for anticipatory proactive security measures, policy enhancements, and improved guidelines to address the root causes for the gaps and build physical and cybersecurity-by-design in connected places.

Chapter 6 provides a summary of the research findings, recommendations, limitations, suggested avenues for future research and the real-world impact of this research.

1.4 Dissemination

Elements of this research (mainly Chapters 4 and 5) were presented in International Congress on Information and Communication Technology (ICICT 2024) conference.

The paper on “Security of connected places” paper (focussed on Chapter 4 and 5) was peer reviewed and published:

Shukla, M. (2024). Security of Connected Places BT - Proceedings of Ninth International Congress on Information and Communication Technology. In X.-S. Yang, R. S. Sherratt, N. Dey, & A. Joshi (Eds.), *Proceedings of Ninth International Congress on Information and Communication Technology ICICT 2024, London, Volume 9* (pp. 195–211). Springer Nature Singapore.
https://link.springer.com/chapter/10.1007/978-981-97-5035-1_15

This research has been presented at multiple conferences and events listed here - Policing 2.0 - Society of Evidence Based Policing (London, Feb 2019), EU Horizon 2020 Project MORE – (Sep 2019, online), Home office talks (online), London Office of Technology and Innovation (LOTI) - (Jan 2021, online), Cyber Science 2023 - Multidisciplinary & Multidimensional Cybersecurity (Jan 2024, Copenhagen), PETRAS National Centre of Excellence London (an institution made of 24 academic universities in the UK) – (Feb, 2024), Ninth International Congress on Information and Communication Technology- London (ICICIT) – (Feb 2024) and, National Cyber Security Show (Sept 2024 at NEC Birmingham, UK). Based on the published paper mentioned above, a policy brief: ‘Strengthening cyber-resilience and procurement frameworks for Connected places’ was also published by **UCL** Department of Science, Technology, Engineering and Public Policy (STeAPP), UK (STeAPP, 2024). This brief was reviewed with the UK Government Departments prior to publication. Elements of Chapter 4 were also included in a deliverable titled ‘Analysis of Technological Advances ([Deliverable 3.1](#))’ for an European Union Horizon 2020 project – ‘Multimodal Optimisation of Roadspace in Europe - MORE’ (MORE project, 2023).

Chapter Two

2 Crime and security in urban places

This chapter is intended to shape the focus for the remainder of the thesis and hence the scope is limited to the impact of urban elements and cyber activities on crime patterns. The aim is to provide a descriptive overview of the principles of crime prevention that have historically informed urban design decisions. A narrative literature review methodology was applied as this methodology is generally used for a comprehensive analysis of a broad topic (Baker, 2016). The chapter begins by discussing theories of environmental criminology that aim to explain why crime occurs where it does, how urban places can shape crime opportunities and the spatial and temporal distribution of crimes in micro places. The chapter then discusses how theories of environmental criminology have been applied to cybercrimes and to the smart environment in connected places.

2.1 Theories of Environmental Criminology

Studies of Environmental Criminology suggest that crime is not random and that crime clusters in time and place (Brantingham & Brantingham, 1995; Sherman et al., 1989), among victims (Pease, 1998) and among facilities (Eck, Clarke, & Guerette, 2007). Motivated by this finding, theories of Environmental Criminology consider the crime event as the object of central interest and place the focus of enquiry on the dynamics of crime events rather than the dispositions of offenders. An important principle of this perspective is that all criminal behaviour results from a person–situation interaction. The immediate environment is not just a passive backdrop for criminal behaviour, but rather it plays a fundamental role in making crime possible and shaping its course. Thus, crime events result not only from criminogenic individuals; they are also caused by criminogenic elements of the crime scene.

Routine Activities Theory

Routine Activities Theory (RAT) assumes that crime can be committed by anyone who has the opportunity (Cohen & Felson, 1979b). RAT states that crime is likely to occur when a motivated offender and vulnerable victim converge in time and space, absent

a capable guardian (Cohen & Felson, 1979; Clarke, 1983). This convergence is proposed to be determined by the everyday movements of victims and offenders and hence, according to the theory, crime will concentrate where the routine movements of victims and offenders overlap. For example, research on routine activities has found that the core daily activities of people, such as hanging out with friends at night clubs, where there is a lack of social control and the absence of authority figures, is positively associated with assault and drug crimes (Miller, 2012). These correlations between routine activities and offenses vary by offence type (Miller, 2012).

Place management

Eck extended the routine activity theory to include place management, visualising concepts using a crime triangle (Figure 2-1), to help researchers understand, address and prevent crime problems (Eck, 2010). The crime triangle (innermost triangle in Figure 2-1) consists of three essential elements that influence criminal opportunity – the offender, target, and place. The next layer includes three crime controllers – handlers, guardians, and place managers; wherein the handler has some influence over the offender, the guardian protects targets/victims, and place managers control the activities at places (Eck, Clarke, & Guerette, 2007). According to this perspective, crime occurs when an offender escapes a handler, finds a target free from a guardian in settings not adequately controlled by a place manager.

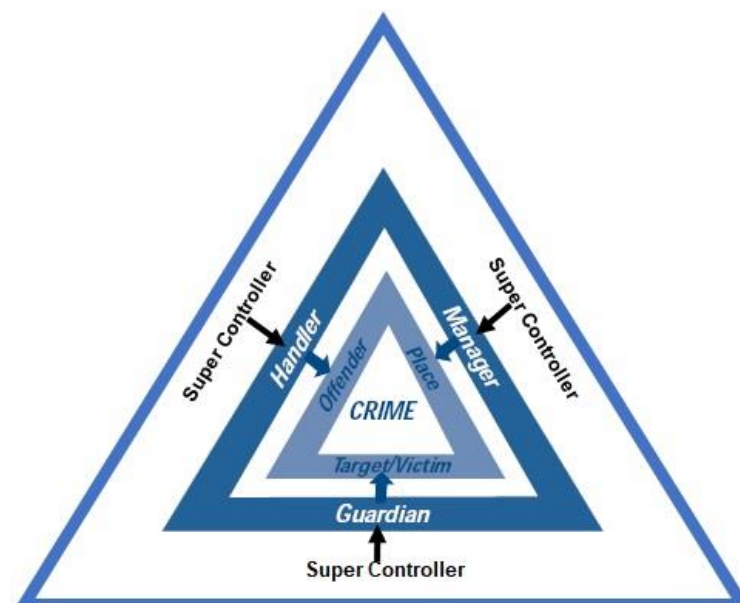


Figure 2-1 Crime Triangle

As seen in Figure 2-1, Sampson et.al (2010) added another layer, that of super controllers. Super controllers are those who can regulate the conduct of controllers. For example, an organizational authority such as security manager may act as a controller, meanwhile, an auditor assessing compliance with regulations on behalf of the Government would be a super controller (Sampson et al., 2010). Super controllers also interact with other super controllers and controllers to prevent crime.

Rational choice perspective

According to the 'The rational choice perspective' (RCP) - offending behaviour is purposive (Clarke & Cornish, 1985) – offenders take cues from the immediate environment to make rational choices by weighing cost and benefit alternatives when considering whether to commit a crime, given an opportunity (Clarke, 1993; Clarke & Cornish, 1985). One of the criticisms of RCP is that it cannot account for decisions made by offenders who commit expressive crimes (e.g., assault, murder, rape) when in state of emotional arousal (anger, fear, jealousy, sexual excitement); wherein the offenders abandon rational choice (Wortley & Mazerolle, 2008). The argument against this criticism is that cost-benefit analysis is involved in expressive crimes too (benefit takes the form of gratification) and although an offender is in an aroused state of mind their decision to harm others 'is a decision nonetheless' (Richard Wortley & Mazerolle, 2008).

Crime Pattern Theory

Crime pattern theory combines RAT and RCP to form a comprehensive meta-theory of crime patterns and helps explain how the built environment, social environment, and people's routine activities contribute to crime. Crime Pattern Theory (Brantingham & Brantingham, 1995) suggests that a crime will occur if an area provides opportunities for crime and it exists within an offender's awareness space. This awareness space is defined by activity nodes (places where people travel to and from for activities e.g., a school, a gymnasium), paths (the routes that people take between nodes) and edges (boundaries of areas where people live, shop, work, etc) (Brantingham & Brantingham, 1995). Offenders move along the street networks that connect people's "routine movement patterns," which include the paths between their activity nodes. This influences an offender's awareness of crime opportunities i.e. suitable targets, vulnerable locations as well as the presence or absence of guardians, at the locations

along the journey (Brantingham & Brantingham, 1995; Frith et al., 2017). Offenders usually travel to the scene of crime, except for crimes such as domestic abuse and cybercrimes (Atkins et al., 1991). According to crime pattern theory, potential offenders tend to search for opportunities to commit crime along the nodes and paths of their own activity and awareness spaces (e.g., relative's home, landmark) (Brantingham & Brantingham, 1995). Zipf's (1949) 'Least effort principle' (Cornish & Clarke, 1987) states that people will usually exert the minimum effort possible to complete their tasks. As a result, offenders typically travel short distances to commit crime, and on familiar pathways not too far from their awareness space (Bernasco, 2010; Kinney et al., 1978; Townsley & Sidebottom, 2010; Vandeviver et al., 2015). In line with this, as evidenced in multiple studies, crimes are likely to occur closer to an offender's home and follow a distance-decay function (DDF) with crimes less likely to occur the further away an offender is from their current or prior home base (Brantingham & Brantingham, 1995; Cornish & Clarke, 1987; Bernasco, 2010). However, the "Journey to crime" literature also notes that offender journeys to offend can be longer depending on multiple factors such as the age of the offender, the type of crime and a perception that higher rewards will be obtained (Townsley & Sidebottom, 2010; Kinney et al., 1978).

Crime is most likely when the awareness and activity spaces of an offender and a victim or target overlap (Brantingham & Brantingham, 1995). As a result, crime hotspots are found at places that may be described as crime generators (activity nodes that pull large number of people towards them resulting in many opportunistic crimes), crime attractors (where offenders are attracted to known crime opportunities) or crime enablers (places with few crime controllers) (Kinney et al., 1978; Kinney et al., 2008). For example, well connected, accessible or frequently travelled street segments such as major roads will tend to have higher crime as they are more likely to fall within an offender's awareness space (Summers & Johnson, 2017). Because criminal behaviour is dependent upon situational factors, crime is patterned according to the location of criminogenic environments. The identification of crime hotspots in time and space can help law enforcement understand the distribution of crime in specific areas and also predict where crimes will occur. It can also guide long-term design, development and the planning of secure urban areas (Chainey et al., 2008).

Situational Crime Prevention (SCP)

Situational Crime Prevention (SCP) derives from the British Home Office's crime-prevention strategy in the 1960s and 1970s (Clarke & Mayhew, 1980; Clarke, 1997). SCP seeks to reduce opportunities for specific forms of crimes by altering the immediate or situational factors in an environment (Clarke, 1983; Eklom, 2017; Welsh & Taheri, 2018). 25 SCP techniques have been developed and these focus on five principles: increasing effort (e.g., controlling access to public buildings using electronic cards), reducing rewards (e.g., disrupting markets selling stolen goods), increasing risks (e.g., utilizing place managers-parking attendants), removing excuses (e.g., labelling "No Parking" signs with clear instructions) and reducing provocations (e.g., efficient queues reducing stressful situations) to reinforce positive behaviour (Clarke, 1983).

Crime Prevention Through Environmental Design (CPTED)

Globally, Crime prevention through Environmental design (CPTED) is an increasingly popular approach to crime prevention that involves manipulating the design and use of the built environment to reduce the fear and incidence of crime (Cozens & Love, 2015; Crowe, 2000). CPTED is a multi-disciplinary approach that engages professionals from disciplines such as architecture, environmental criminology, planning, law enforcement and environmental psychology, to inform the design and management of the built environment to reduce crime and the fear of crime (Schubert, 2016; Gibson & Johnson, 2016; Armitage & Monchuk, 2019a; Cozens & Love, 2015b; Atlas, 2008). The origins of CPTED trace back to criminologist C. Ray Jeffery, urban planners Jane Jacobs and Oscar Newman. C. Ray Jeffery developed the original ideas and coined the term CPTED (Jeffery, 1969; Jeffery, 1971), Jane Jacobs (Jacobs, 2000) discussed the fact that land use diversity provided more 'eyes on the street' (surveillance), while Oscar Newman (Newman, 1972) suggested that architectural and environmental design plays a crucial part in increasing or reducing criminality. According to Newman, residents can be motivated to improve surveillance opportunities to deter offenders and control their environment if the "ownership" of spaces is clearly defined; which was termed as "defensible space" (Newman, 1972). The concept of defensible space extends Jacob's ideas for crime deterrence through natural surveillance. CPTED principles, amongst other security-by-design principles, have been embedded in building regulations (Cozens & Love, 2015) and national as well as regional planning policy frameworks in countries including South Africa,

Netherlands and Australia (Manual for Streets, 2007; Irvin-Erickson, 2015; Clancey, Lee, & Fisher, 2012). The CPTED crime prevention approach has also gained the support of the United Nations (Cozens & Love, 2015).

Early CPTED ideas for a secure area, termed 'First-Generation CPTED' consisted of seven principles (Ekblom, 2011a; Cozens & Love, 2015) - territoriality, surveillance, activity support, access control, target hardening, image management and geographic juxtaposition. Activity support is about providing a safe environment for people's activities. For example, a safe private space provided to individuals for cash transactions at an Automatic Teller Machine (ATM) encourages acceptable behaviour. Crime risks are considered to be high when products and services such as an ATM are introduced and used heavily by people, but potential vulnerabilities have not yet been identified or addressed, making them a suitable target for criminals (Guerette & Clarke, 2003). Target hardening is achieved by limiting unauthorized access and thereby increasing the effort an offender would be required to expend to reach a target. A physical security guard or a mechanical device such as a lock can achieve this in some situations. However, with some of these approaches, there is a danger of creating a "fortress" mentality if target hardening, for example, is not implemented proportionately (Clarke, 1983). Image management refers to designs that support easy maintenance, which has been an under-researched area (Ekblom, 2011a; Peršak, 2021). Geographical juxtaposition is a concept where the safety and security of an area is affected by the level of unsafe or insecure activities in adjacent areas (Clarke, 1993; Newman, 1972). For example, bars may result in criminal activity in areas that surround them. CPTED principles have been built into physical security regulations such as building and road regulations, however, critics have claimed that these focus mainly on increasing territorial control (Cozens & Love, 2015).

CPTED evolved to include wider elements of the environment, community culture (encouraging a strong sense of community to act collectively on shared goals), and threshold capacity (creating capacity for activities and land use). This evolution was termed 'Second-Generation CPTED' (Cozens & Love, 2015; Cozens et al., 2005; Sampson et al., 1997; Sánchez Salinas & Fuentes Flores, 2016). While first generation CPTED encourages design strategies to keep offenders away from victims and targets, second generation CPTED focuses on preventing crime from growing in communities and neighbourhoods by focusing on social issues and situational factors

(Mcglinn et al., 2011). Researchers suggest that the principles of first and second generation CPTED can be expanded further to integrate people's motivation to make the neighborhood more livable– this is termed third generation CPTED (Mihinjac & Saville, 2019).

Third Generation CPTED thus takes a still more holistic approach to foster a quality of life based not just on secure places and services but also personal goals (Cozens & Love, 2015; Mihinjac & Saville, 2019). It focuses on embracing 21st century advances such as sustainability goals (e.g., inclusivity and greenery); people's perception of a good environment and the integration of information and crime sciences with liveability to provide a good quality of life (Cozens, 2002; Lacinák & Ristvej, 2017; Prislán & Slak, 2018; Saville & Mihinjac, 2022).

Research and reviews of case studies have provided evidence that CPTED implementation applied in urban settings such as buildings, car parks, transport, transit, greenery and retail facilities can reduce crime as well as fear of crime (Cozens & Love, 2015). The basic principles of security-by-design that CPTED encapsulates are practiced by a few local, regional and national building and city planning authorities world-wide (Irvin-Erickson, 2015). For example, security-by-design principles are embedded in anti-terror interventions to protect the street security (Cozens & Love, 2015). In several boroughs in the UK (e.g., Greater Manchester), it is mandatory for urban planners to review security risks with security consultants prior to the planning approval of an urban element (e.g., building, road) to ensure that secure measures are embedded within the design (Davey & Wootton, 2016; Hirschfield et al., 2001; pbctoday, 2017). Another example is that CPTED principles are embedded in the urban planning guidelines and regulations of the US department of Justice (Schneider, 2005). CPTED implementation based on the local context enables the assessment of local crime risks and is thought to be more effective than interventions based on CPTED principles applied without sufficient local context (Clancey et al., 2012; Cozens et al., 2019).

One of the criticisms of crime prevention approaches including SCP and CPTED is that they merely displace crime into other areas, to a different time, to a different target, or the offender changes the tactics used in offending, or switches to a different type of offence (Cozens & Love, 2015b; Johnson et al., 2014; Barr & Pease, 1990; Cornish & Clarke, 1987). Perpetrator displacement can also occur when new offenders replace those who have been deterred, taking over the criminal activity

(Guerette & Bowers, 2009). However, research findings indicate that crime reduction using SCP and CPTED principles can extend positively in surroundings, which is termed a diffusion of benefit or “Halo effect” – opposite effect of displacement (Bowers et al., 2011; Guerette & Bowers, 2009). The two can also co-occur. Guerette & Bowers (2009) studied displacement and diffusion effects in 102 SCP projects and found that displacement and diffusion of benefits occurred in almost the same number of studies (Guerette & Bowers, 2009). In the event of crime displacement, a diffusion of crime control benefit, can also possibly outweigh any crime displacement effects (Bowers et al., 2011; Telep et al., 2014; Weisburd et al., 2006; Green, 1995; Johnson et al., 2014).

Although third generation CPTED is intended to address the shortcomings of prior CPTED principles – such as lack of a human centric solution – there is criticism about a lack of availability of integrated solutions to achieve the objective (Mihinjac & Saville, 2019). Cozens et al. (2019) argue that the greatest impediment to the widespread use of CPTED is ignorance and a lack of unity in technical approaches resulting in its inconsistent application across locations (Cozens et al., 2019). For example, efforts to implement a standardised approach to CPTED delivery across Europe have not been successful (Stummvoll, 2012). Although CPTED principles are included in planning policy and guidance for crime prevention, there are instances observed in Europe, Canada and the USA, that Crime Prevention Officers are not engaged at the right point in time (if at all), and planners and urban designers are not involved consistently which can lead to implementation failures (Ekblom, 2011b; Clancey et al., 2018). Crime prevention interventions need to go beyond anticipation and risk management by working with communities to create safe and secure urban design policies with universally accepted frameworks (Clancey et al., 2018; Johnson et al., 2014; Butler, 2013).

2.2 Physical crime concentration in urban places

Research suggests that that urban crime patterns are correlated with the design of places (Crowe, 2000). The choice and placement of land use elements such as roads, bridges, tunnels, buildings and walk ways play an important role in determining the routine movement patterns of individuals (Wuschke & Kinney, 2018; Kinney et al., 1978). Street configuration and connectivity shapes land uses and how people move as well as interact within urban spaces which can also affect crime opportunities (Davies & Johnson, 2015; Summers & Johnson, 2017). Crime opportunities in urban

spaces are shaped by one or more factors such as land use, characteristics of the built environment, street network patterns, people's activities, natural or installed interventions and sociodemographic changes (Adel et al., 2016). Land use shapes the spatial distribution and patterns of urban crime by facilitating the convergence in space and time of offenders and suitable targets, in the absence of capable guardians (Cohen & Felson, 1979a; Rondeau et al., 2005; Wuschke & Kinney, 2018).

Empirical research suggests that crime risk varies within and across types of land use categories, and that specific land use types are more criminogenic than others due to their physical and social characteristics (Eck & Weisburd, 1995; Irvin-Erickson, 2015; Kennedy, Caplan, & Piza, 2011). For example, the use of permeable street network designs in mixed land use areas can facilitate varied movement patterns and hence can be associated with higher levels of crimes (Sohn, 2015). Connected streets and areas with higher accessibility, high traffic and those that are frequently travelled correlate with a higher concentration of targets and increased offender awareness; and hence higher crime (Newman, 1972; Beavon et al., 1994). In contrast to through roads, cul-de-sacs have lower connectivity and hence are less likely to be used; the true cul-de-sac (with the least connectivity) is a stronger defensible space, followed by the through road and the leaky cul-de-sac (Armitage, 2011). On less connected streets, strangers are likely to be easier to detect by locals and offenders are less likely to come to know these street segments (unless they live on them). Inadequate street lighting placement can leave dark areas at street corners providing opportunities for violence, disorder and drug crimes (Farrington & Welsh, 2002; Weisburd et al., 2016a; Xu et al., 2018). Mixed land uses such as industrial, office and retail stores, shopping malls, eating establishments and entertainment venues can result in a more diverse environment resulting in more people on the street that provide natural surveillance to reduce crime. In the same manner, a high density of pedestrians, street layouts that encourage walking and the flow of vehicles on the street provide security in the form of "eyes on the street" (Ceccato, 2012). On the other hand, these same features might attract too many people resulting in the loss of a sense of ownership and social control, which might increase crime (Clancey et al., 2018; Cozens & Love, 2015b; Cozens, Love, & Davern, 2019). The prevalence of crime, public fear of crime, and the types of offenses committed have been shown to differ depending on the location of public transit stops (Qin & Liu, 2016; Smith, 2008; Sung-suk & Smith, 2014).

Three other concepts that describe how facilities or land use might influence crime a) Crime detractors i.e. places that detract people can result in the use of the place by offenders, for example an unlit corner where drugs are sold (Kinney et al., 2008). b) Crime facilitators i.e. things that enhance the capabilities of offenders, for example use of drugs (Clarke, 2005) ; and c) Situational crime precipitators i.e. situational aggravators that exist in the environment resulting in crime, for example a long queue on a hot day (Wortley & Mazerolle, 2008). In summary, research suggests that the choice of land use in urban design that leads to its effective utilization can contribute to lower crime rates and a good quality of life for people (Crowe, 2000). The redesign of the built environment such as sufficient street lighting, widening footways to add benches for people, and the maintenance of public transit stops can deter criminal activity and provide a safe street environment for people.

According to Weisburd's 'law of crime concentration at places', crime concentrates in a stable and consistent manner at small urban micro places (Weisburd, 2015). Research suggests that a small proportion of micro places, also known as “hot spots” of crime, that may be either crime attractors (i.e. places that attract motivated offenders) or crime generators (i.e. places that attract many people which creates criminal opportunity) tend to be associated with a large proportion of overall crime (Brantingham & Brantingham, 1995; Cozens & Love, 2015; Farrell & Pease, 2010; Weisburd, 2015). Additionally, repeat victimisation may occur because of a victim or target's vulnerability that the offenders find attractive, hence in a small number of victims (people or targets) account for a large amount of victimisation (Clarke & Weisburd, 1994; Eck, Clarke, & Guerette, 2007; Farrell & Pease, 2010; Pease, 1998). This unequal distribution of crime closely aligns with the Pareto principle, or the 80-20 rule, which suggests that 80% of urban crimes occur in just 20% of urban spaces (Eck, Clarke, & Guerette, 2007). Research evidence has supported this 80-20 rule, showing that a small number of locations—such as railway stations, hospitals, and parking lots—where offenders, victims, targets, and place managers may change over time, contribute to a disproportionately large share of crime (Eck, Clarke, Guerette, et al., 2007).

Once an offence has been committed, the probability of offenders choosing their targets with similar features , on similar days, locations and times is very high (van Sleeuwen et al., 2018). The crime rates associated with some facilities such as (alcohol outlets, shopping complexes, pawn shops, restaurants, hospitals and

recreation centres) are disproportionate compared to other facilities even during the times they are closed (Wuschke & Kinney, 2018; Irvin-Erickson, 2015). After a nightclub closes, crime might still occur if drunk people linger in the area. Crime concentration, meaning high levels of crime clustered in a place, is caused by a variety of reasons. The absence of controllers such as guardians, handlers, and managers as well as lack of informal social surveillance such as “eyes on the street” may contribute to crime concentration (Eck, 2010). The clustering of crime increases further if many offenders are located in a geographical area and there are many attractive targets available (Weisburd et al., 2016b). Research shows that although a neighbourhood might have a high overall crime rate, the entire neighbourhood need not be criminogenic (Herrmann, 2015). For example, it has been observed that some transit stops have very little incidence of crime, even when others in close proximity to them and along the same bus routes have high crime rates (Loukaitou-Sideris, 2012).

Crime is distributed across a range of geographical units from neighbourhoods, to individual addresses (Johnson & Bowers, 2010b; Groff & Lockwood, 2014). Since the early twentieth century, research on crime patterns at places has shifted from a focus on macro places (e.g. cities, census tracts, neighbourhoods) to micro places (e.g. street segments) (Weisburd, 2015). Micro places range from census blocks, single or small groups of clusters of addresses, street segments, particular street intersections, and grid cells. The definition of these units differs from country to country, and this is important to discuss to provide a context for what follows in subsequent chapters. As shown in Figure 2-2, in the US, the census geography hierarchy for a state includes the county, census tract, census block groups and census block, where the county is the largest geographical unit, and the census block is the smallest. To provide an indication of the size of these units, the population of a US Census tract is between 1,000 and 8,000 people, with an average of 4,000 people and the census block groups have a population of 600 to 3,000 people (Census Information, 2010). Census blocks (with a population of 0-600 people) are defined as the four block faces of a square street block i.e. bounded on all four sides by streets and its population can vary (Weisburd, Groff, & Yang, 2012; Census Information, 2010). The Canadian census neighborhood hierarchy includes the census tract (with a population of 2,500 to 8,000 residents), dissemination area (with a population of 400 to 700 residents) and dissemination block (area equivalent to a city block bounded by intersecting streets (i.e., streets on 4 sides) (Sánchez & Fuentes, 2016). In Australia,

the census hierarchy of geographic units in a state (Australian Bureau of Statistics, 2016) include a) Statistical Area (SA) Level 4 (population more than 100,000 but less than 500,000), b) SA Level 3 (population more than 30,000 but less than 130,000), c) SA Level 2 (population more than 3,000 but less than 25,000), d) SA Level 1 (population more than 200 but less than 800) and; d) mesh blocks (with 60 to 80 residents or 30 to 60 dwellings-surrounded by intersecting streets). In New Zealand, the hierarchy of census geographical units within an urban area consists of Statistical Areas (SA) 2 (residents more than 1000 and less than 4000), SA1 (100-200 residents or up to 500 in urban areas) and mesh blocks (60-120 residents) (Stats NZ, 2018).

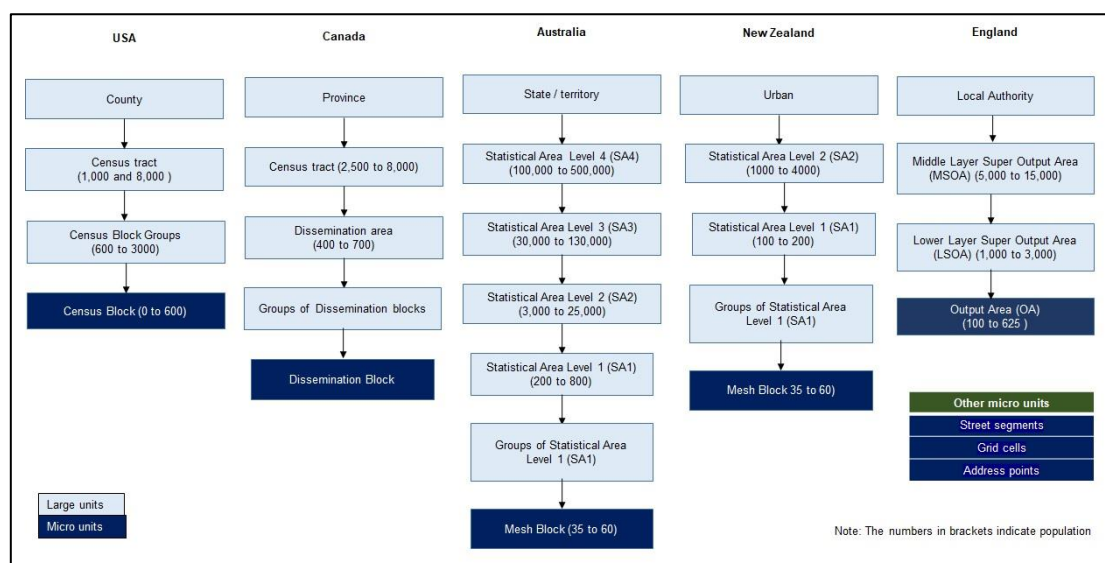


Figure 2-2 Hierarchy of spatial units

England's Census Geography hierarchy includes counties (local authorities), Local Authority Middle Layer Super Output Area (MSOA), Lower Layer Super Output Area (LSOA) and Output Areas (OA), where a county is the largest geographical unit, and the OA is the smallest. The population of UK's MSOAs range from 5000 to 15,000 people or 2000 to 6,000 households (Office for National Statistics-a, 2011). The population of LSOA ranges from 1000 to 3,000 people or 400 to 1,200 households, and the OA is composed of 40 to 250 resident households or 100 to 625 resident people (Office for National Statistics-a, 2011). Researchers use census tracts and the aggregation of census blocks, dissemination areas, output areas and mesh blocks to analyse larger geographical areas. For example, statistical divisions of census tracts termed block groups are sometimes used as a spatial unit of analysis. These block

groups generally consist of between 600 and 3,000 people (Census Information, 2010).

Grid cells are also sometimes used as micro spatial units as an alternative to other units (Rosser et al., 2017) e.g. 50mx50m grid cells. The grid cell as the spatial unit of analysis is advantageous as the grid cells have fixed dimensions, whereas this is not the case for other units of analysis. Hence, it standardizes the content from a geographical point of view. However, analysis using such a unit may not provide the intended outcome if the composition of cells differs massively in terms of number of streets or households. The Office of National Statistics also provides street segment data for the UK as well as address point data, which allows for the analysis of crime based on the count of homes at the street segment level. A street segment is defined as 2 block faces on both sides of a street between two intersections (Weisburd et al., 2012). A block-face is one side of a street between two consecutive features intersecting that street. The street intersection is where two or more streets cross. The length of street segments varies across cities and countries, but is often 800 feet in length, and typically less than 1,600 feet (Weisburd et al., 2009). Findings from studies of crime on street segments have provided insight into the street-to-street distribution of crime patterns. For example, Weisburd, Groff & Yang (2012) found that half of all urban crime in Seattle occurred on 5% of street segments (Weisburd et al., 2012).

The limitations of using small spatial units such as street segments include a) difficulties in obtaining crime data, and b) socio-demographic data affecting crime rates at street segment level is available only at larger census-based units (Groff, Weisburd, & Yang, 2010; Taylor, 1997). Hot spot analysis examines how crime events are concentrated at specific targets and locations using one spatial unit of analysis or another (Sherman et al., 1989). Research concerned with repeat victimization of the same people (Farrell & Pease, 2010; Pease, 1998) and places (Bernasco et al., 2015; Eck, Clarke, & Guerette, 2007; Levy & Tartaro, 2010; Pitcher & Johnson, 2011) illustrates that crime is concentrated at even smaller units of analysis than street segments. Crime mapping, and the use of geographic information systems (GIS) has helped to automate analyses of crime concentration, and the outputs have been used by the police to identify crime hot spots where efforts can be focused for crime reduction (Haberman, Sorg, & Ratcliffe, 2017; Chainey & Ratcliffe, 2005). Researchers have developed models to predict the crime risk of a place (Rosser et al., 2017a; Bowers et al., 2004) with the aim of allowing police services to anticipate the

locations of future crime events (Bowers et al., 2004). Qualitative and quantitative research provides evidence that crime opportunities and thus, offending can be reduced through better environmental design, urban planning, managing situational factors and security interventions (Davey & Wootton, 2016; Jongejan & Woldendorp, 1978; Monchuk & Clancey, 2013). A large number of studies have explored the CPTED principle of security-by-design in urban places (such as building regulations, CCTV for surveillance, property marking, access control mechanisms, lighting, street closures to reduce congestion, and alarms) and the effectiveness of these measures (Eck & Guerette, 2012).

To summarise, extensive research on crime and place that have implications for preventing future crime risks has focussed on criminogenic features of the urban built environment, crime concentration at specific locations in a neighbourhood; features of urban elements that can prevent crime, rational thinking behind how offenders select their targets, spatio-temporal analysis of crime patterns and place management. A preliminary search of the literature was conducted for qualitative and quantitative effects of built environment on crime. The results suggest that there is a need for more systematic reviews that analyse effect-sizes of criminogenic urban elements using micro units (Further evidence-based analysis is conducted in Chapter 3).

2.3 Environmental criminology and cyber crime

Theories of environmental criminology were originally formulated to explore urban crime and security in physical spaces. However, traditional criminological theories may still be applicable for analysing and understanding cybercrime.

RAT and RCP

Although offenders do not need to travel physical distances to commit cybercrimes, human behaviour is subject to routine activity patterns in virtual environments too. A number of studies have applied RAT and RCP to cybercrimes including phishing, unauthorized access of computer systems, fraud, malware infection, identity theft, computer viruses, cyber bullying, and cyber stalking (Howell et al., 2017; Hsieh & Wang, 2018; Vakhitova et al., 2016; Zhang et al., 2022; Zhon & Asiana, 2022). Research suggests that carrying out certain online routine activities is related to specific forms of cybercrime: online banking, shopping, messaging, and downloading all appear to be associated with an increased likelihood of identity theft (Reyns, 2010); downloading, and using dating sites seems to favour victimization by

malware infection (Holt et al., 2020); and online shopping may be associated with experiencing consumer fraud (Wilsem, 2011). Individual users' routine activities are reflected in their communication patterns such as those that take place on social media. E.g., A research that analysed the association between local assaults, robberies and burglaries (across nine cities in the USA) with interests marked by people from a zip code on facebook, found that people's interests marked on facebook support prediction of crime rates (Fatehkia et al., 2019).

Research on cybercrimes such as romance fraud on dating websites, online blackmail, ransomware, sextortion, darknet market fraud indicate that a large proportion of cybercrimes are associated with a small number of active online identities (Buil-Gil & Saldaña-Taboada, 2022). Research by Ding et. al (2019) established a relationship between online search data, Taobao bicycle sales data and theft of bicycle theft in China (Ding et al., 2019). Rege (2014) researched cyber-attacks on the industrial control systems of power plants and found that the offenders engage in research prior to making active rational choices based on the system's environment (vulnerabilities of the target), guardianship (quality of measures to prevent cyber-physical attacks) and capabilities (alliances and skills) built by the offenders (Rege, 2014). However, Butkovic et al.(2019) suggests that applying RCP to cybercrimes is challenging due to difficulty in understanding the cyberspace, difficulty in locating the crime-scene, quality and diversity of data, and offenders quickly adapting their modus operandi to reorganise based on security/technology advancements (Butkovic et al., 2019; Ladegaard, 2019).

Cyber place management

Criminologists and crime practitioners have applied place management techniques to prevent not just potential physical crime events but also crime events in virtual domains with contrasting results. Each cyber place requires a customised security strategy and a set of controllers – handlers, guardians and place managers. The handlers could be same as in the physical world – people who influence offenders and prevent them from reaching targets. Felson defined the role of guardians as anyone who can keep an eye on the target (Hollis-Peel et al., 2011) and hence they could be citizens who report an offender's online conduct, online administrators or security personnel who deny access to a website if valid credentials are not provided

(Vakhitova et al., 2016). For example, in case of websites with large numbers of people live streaming content, the greater the website traffic, the greater the guardianship. While guardianship may prove effective in preventing certain crimes on privately owned sites, online tools that can be used by anyone may not be secure; hence internet service providers play a fundamental role in controlling e-commerce crime (Hsieh & Wang, 2018). Reyns (2010) argues that if digital environments such as websites are cyber places, *“then website administrators, webmasters and designers are their place managers”*(page 104) (Reyns, 2010). Cyber place managers *“can manipulate the online environment at will, limit access, and set rules for participation in the site”* (page 105) (Reyns, 2010) . Place managers can protect cyberspaces through measures including good cybersecurity training to improve the capabilities of service providers, enforce codes of conduct defined by them and implement preventive security measures (Back & Guerette, 2021). One of the reasons for a lack of effective cybersecurity, guardianship and place management is the large number of vulnerabilities due to which *“any protection measure is only being as strong as its weakest link.”* (Hsieh & Wang, 2018). For example, Back & Guerette (2021) analyzed the effectiveness of one place management measure - cybersecurity awareness training imparted to employees to prevent cyber-attacks and found that this was limited, as despite the trainings received, victimisation was higher for employees who had higher levels of online exposure (Back & Guerette, 2021).

Governments across the world, as super controllers have implemented legislations to deal with cybercrimes. Many countries including the USA, China, EU and NATO countries have called for increased resilience in services through the delivery of mature cybersecurity capabilities that are informed by the analysis of patterns of cybercrime (NIST, 2018; Maglaras, Drivas, Noou, & Rallis, 2018; Štitilis, Pakutinskis, & Malinauskait, 2017). However, this has proved difficult to implement as organizations have historically been hesitant to report most types of victimization, and there is insufficient governance, which makes it difficult to analyse patterns of cybercrime (Schneier, 2015; Shukla et al., 2019).

CPTED and SCP

Few studies have critically evaluated the crime prevention principles such as access control, natural surveillance and control that are included in the information security standard ISO27001 to critically evaluate the implications of CPTED for cyberspaces

(Howell et al., 2017; Lee et al., 2020; Lim, 2021; Remrey & Maimon, 2016). In cyberspaces, CPTED strategies can mitigate hacking events by reducing the likelihood of hackers accessing a previously hacked environment (Fisher et al., 2022). Lee et al (2020) suggested how to apply spatial analysis, determine territorial controls and identify criminogenic cyberspace designs using CPTED principles (Lee et al., 2020). Although security policies enhance security system maintenance, there is limited research to assess the effectiveness of crime prevention concepts applied to the cyber world (Lim, 2021). The CPTED concept of Security-by-design for cybercrime prevention and curbing crime harvests (see Chapter1, Section 1.1.4) is a popular concept, the application of which needs to adapt to continuous changing technological innovations (Joo et al., 2018).

With the global increase in cyber security challenges (Blythe & Johnson, 2021; Burke et al., 2024; Heidari et al., 2023; Langer & Kammerstetter, 2015; Saeed et al., 2023; Staniforth, 2013; Weber & Studer, 2016), practitioners and researchers are increasingly investigating opportunities for applying SCP and CPTED principles by gathering insights into how offenders (and potential victims) interact with digital environments and how this generates opportunities for cyber-attacks (Schneier, 2015). Methods applied for information security in organizations to help develop deterrence and the prevention strategies in the online environment have been studied by researchers from the SCP perspective (Hinduja & Kooi, 2013; Ho et al., 2022; Reyns, 2010). Below are examples from the literature for each of the five SCP techniques where environmental criminology principles have been applied.

a) **Increase effort:** This technique focuses on making it harder for potential offenders to commit a crime. Known vulnerabilities in digital systems that provide an easy way for hackers to infect the systems include unpatched devices (i.e. where devices are not updated with software patches that address identified vulnerabilities), weak encryption, weak passwords, and outdated firmware (Anderson, 2008; Cheng, 2011; Chris Lewis Group, 2021; Ho et al., 2022; Labus, 2022; Zhao et al., 2017). Research on this technique includes limited interventions such as the public shaming of ISPs, taking down offending domains, alerting people about suspicious websites and mandating change of default passwords provided by the manufacturers (Ho et al., 2022). For example, in 2023, the Cybersecurity and Infrastructure Security Agency (CISA) in the USA raised an alert that Iranian threat actors gained access to Critical National Infrastructure (CNI) using default

passwords (Daws, 2023). The Department of Science Technology and Innovation (DSIT), UK also provided guidelines for security-by-design which included manufacturers disabling or forcing a change to default passwords (DSIT, 2019a; Government-a, 2017). Other examples of security interventions include good encryption, the use of system patching to address known vulnerabilities, antivirus software, the regular updating of firmware, limiting third party access, spreading awareness, and other basic security health checks (Anderson, 2008; Cheng, 2011; Chris Lewis Group, 2021; Ho et al., 2022; Labus, 2022; Zhao et al., 2017). The strengthening of surveillance and introducing additional authentication steps has also been shown to increase the efforts of committing financial crimes (Zaharia et al., 2010).

- b) **Increase the risks:** This technique aims to increase the likelihood of offenders being detected. SCP techniques include utilising on-line place managers and extending guardianship to increase the risks of committing crime. Studies that analysed cyberstalking and computer fraud through the lens of routine activities theory found that the presence of on-line cyberplace managers and other responsible users on the system (extends guardianship) increased the chances of unusual activities of the offenders being reported and helped protect the victims (Remrey & Maimon, 2016; Reyns, 2010). Other interventions include application of popular industry standards such as ISO/IEC 27002 (Ho et al., 2022).
- c) **Reduce rewards** - This technique aims to reduce the benefits or rewards criminals gain from committing a crime. Researchers have used false websites to observe illegal activity and attract criminals with an aim of disrupting illegal dark web markets. Honey pots (online systems set up as a decoy to lure cyber attackers) have been used by undercover agents to bust underground dark web markets such as the Silk Road (Levi et al., 2017) and Hansa (Ho et al., 2022). Other interventions under this the SCP technique include but are not limited to denying benefits by penalising malicious search at offending internet service providers (Ho et al., 2022).
- d) **Remove excuses** – This technique aims to eliminate excuses for committing crime by increasing awareness of laws, rules, and norms. Displaying a warning banner that threatens law enforcement actions as soon as a hacker gains access to a system has been shown to deter cyber-trespassing events (Howell et al., 2017). Online warnings have also been found to act as a deterrent on websites with inappropriate material (Prichard et al., 2024). Other interventions include

awareness trainings (to educate users about the cybercrime risks and safety/security measures), and publishing policies on websites (such as modern slavery, privacy protection, code of Ethics) (Back & Guerette, 2021; Ho et al., 2022)

e) **Reduce provocations** – This technique focuses on minimizing situations or environmental factors that may trigger criminal behaviour. Research on this technique includes interventions to include emotional arousal, e.g. online platforms employ content moderation algorithms to identify hate crimes/ racially aggravated messages/ fake content, and social media administrators could ban users who post inappropriate content (Myers West, 2018).

Although research papers have proposed how SCP techniques can be applied to cybercrimes and limited research has assessed individual interventions, more work is required to analyse the effectiveness of all SCP techniques in preventing cybercrimes (Back & Guerette, 2021; Blythe & Johnson, 2021; Ho et al., 2022; Vakhitova et al., 2016). Mainstream criminology needs to conduct more research on victims and offenders of cybercrime to advance criminological theory in the changing nature of crimes (Maimon & Louderback, 2019). A preliminary search of the literature conducted about the effects of people's cyber activities that are related to the built environment on crime suggests that more research is required in this specific area (Further evidence-based analysis is conducted in Chapter 3). For example, residents sharing anomalies/ observations about their neighbourhood on a website alerting residents and police or people share their real-time location/holiday pictures on social media which could motivate burglars to commit crimes (Bendler et al., 2014). The literature is full of controversy as to whether environmental criminology theories can be adjusted easily to explain cybercrimes or whether the theories need re-evaluation due to major differences between cyber and traditional physical environments as well as methods to commit crimes (Smith & Stamatakis, 2020). Physical and cybersecurity approaches, frameworks, and regulations need further integration (Miró Llinares & Johnson, 2018a).

2.4 Environmental criminology - Crimes in connected places

While the redesign of streets to include digital elements and advanced technologies may make city infrastructure more efficient, it may also create new opportunities to commit high impact crimes remotely (Shaw, 2016; Ahmed & Rani, 2018; Pribyl &

Pribyl, 2015; Prislán & Slak, 2018). The urban elements of the street environment that constitute places on the street are changing to include smart elements such as smart roads with lane markings that communicate with smart vehicles, smart streetlights, smart buildings, smart garbage bins, digital kiosks, public wifi, smart CCTVs and smart transit. IoT, 5G mobile, big data, and Artificial Intelligence (AI) applied to smart infrastructure have led to the use of cyber-physical systems connected to other smart infrastructure systems resulting in a much larger attack surface for CNI. Additionally, it is very challenging to manage the risks of cascading impacts (see Chapter 1, section 1.1.4) to the CNI because a) the physical and cyber systems within smart systems including CNI are inter-connected and inter-dependent and b) Smart services including CNI services are now controlled / operated by cyber systems (Schauer et al., 2019). Inter-dependencies across systems including CNI (such as water treatment plants and water distribution systems) in connected places make them an attractive target for cyber-attacks (Palleti et al., 2021). Some studies have analysed cascading impacts, such as power outages, resulting from cyber-attacks on Electric Vehicles (EVs) integrated with smart grid infrastructure. (Acharya et al., 2020; Johnson et al., 2022; NESCOR, 2015). However, research is lagging on place management and the effectiveness of security measures to prevent such cascading impacts across cyber and physical entities in connected places. The holistic security across cyber and physical spaces is shared across law Enforcement, regulators, Government, businesses, community, and citizens. ‘Security and resilience by design’ are both applied to physical and cybersecurity by professionals from different disciplines. In the UK, the Center for Protection of National Infrastructure (CPNI) (now NPSA- National Protective Security Authority) and the NCSC are working towards a holistic (integration of physical security, people security and cyber-security in the context of smart solutions) approach (Shukla et al., 2019); the Home Office defines the strategic approach for holistic security enforcement through the collaboration of entities; whereas one of the DSIT’s key functions is to ensure a secure deployment of technological solutions (DSIT, 2023). However, it is also important to assess how accountabilities and governance are designed to address the security of connected places, for city authorities and urban planners to transform them into defensible spaces (Miró Llinares & Johnson, 2018b).

For crime prevention to be effective, it is important to study the continuously changing urban environment, its influence on people’s behaviours as

they adapt to the new technological innovations, and to anticipate how crime opportunities emerge (Miró Llinares & Johnson, 2018b). There is research on how environmental criminology theories apply to smart environments, the crimes that might evolve and security interventions, but it is limited to specific scenarios and does not provide a holistic application framework. To illustrate, a few examples are provided here. Researchers have studied how criminal activity can be deterred by promoting the CPTED principle of surveillance by improving performance and location of smart lights and smart cameras (Cho et al., 2019; Lee et al., 2019). Studies have also supported how CPTED principles could help measure risk of leakage of sensitive information (Joo et al., 2018) and crime prediction using AI-enabled image recognition algorithms and big analytics (i.e. methods to collect large, complex and diverse urban data) (Moon et al., 2014; Vogiatzaki et al., 2020).

Digital policing initiatives focus on specific projects such as facial recognition that support real-time detection of an offender, however, these interventions could cause harm due to bias and computer errors (Benedict, 2022; Eveleth, 2016; Somani et al., 2023). CPTED will increasingly rely on connected digital infrastructures and there is a need for more proactive practices based on the changing digital security model of law enforcement (Ghappour et al., 2017; Weber & Studer, 2016). The sustainability, scalability and continuous adaptation as well as effectiveness of CPTED will only be achieved through crime prevention principles being a part of the day-to-day activities, roles, responsibilities of multi-disciplinary professionals and organizational culture (Ekblom, 2011; Davey, 2016; Armitage & Monchuk, 2019a). Armitage suggests that CPTED principles and practices need re-assessment and the CPTED applications need to evolve (Armitage, 2018). Crime prevention interventions need to go beyond anticipation and risk management by working with communities to create safe and secure urban design policies with universally accepted frameworks (Clancey et al., 2018; Johnson et al., 2014; Butler, 2013). Modern technological innovations, such as those associated with connected places, are expected to further transform the built environment and crimes in smart environments demanding the adaptation of environmental criminology principles (Back & Guerette, 2021; Cozens et al., 2019; Gupta et al., 2018; Ho et al., 2022; Remrey & Maimon, 2016).

Research is lagging behind in terms of understanding the impact of crimes associated with urban IoT systems connected on an enormous scale, and how crime patterns are changing from those observed for “traditional” physical and cybercrimes

(Ekblom, 2011a, 2011b; Joo et al., 2018; Rejeb et al., 2022; Rohit Sharma & Arya, 2023). There are also research gaps in the field of understanding vulnerability and security measures for urban IoT systems (Barau, 2016; Vermesan et al., 2020). A preliminary search of the literature suggests that there is very little research on the impacts of all these new urban elements and the integrated smart services that is changing the urban landscape, movement and activities. Although there is research on crime impacts and security measures in smart environments, it is limited to individual smart systems, interventions and uses rather than the collective impacts in connected urban places where multiple cross-sector smart infrastructures operate.

2.5 Summary

The review initially discussed theoretical perspectives regarding the physical crime concentration at places, and how urban design and land use diversity generates physical crime opportunities. This was followed by a consideration of how spatio-temporal patterns of crime in built environments are influenced by urban elements, crime prevention techniques and empirical research that has tested these. The review then focussed on how the use of technological applications in the built environment and day-to-day lives of the people influence changes in cybercrime. Examples of environmental criminology principles applied to cybercrimes such as security-by-design advocated by SCP were described. Finally, the review discussed the research gaps in assessing the changing nature of crimes in digitally connected places using principles of Environmental Criminology. Three clear findings emerged from searching the literature which support the aim of this thesis.

First, the built environment (physical or cyber) shapes crime opportunity; and changing urban environments influence crime and security landscapes. Decades of empirical research demonstrate that crime is concentrated at a range of spatial scales, from neighbourhoods, to smaller places such as street corners, zip codes, census blocks, street segments, buildings and individual addresses (Johnson & Bowers, 2010). However, the choice of the spatial unit of analysis has played a particularly critical role in research and geographic analysis of crimes (Eck & Weisburd, 1995; Weisburd et al., 2009). The study of physical spatio-temporal crime patterns in micro places identifies crime patterns associated with the local environment and behaviours more accurately. Studies that provide quantitative analysis of such spatio-temporal crime patterns not just in physical spaces but also in cyberspaces (with geo-

tagged data) could provide inputs to urban planners for better urban designs that could reduce physical crime opportunities. However, there are very few systematic literature reviews that analyse the quantitative effects of urban elements on crime in micro places. More research is also required on human activities related to cyber spaces within the urban environment and its impact on physical crime in micro places. It is important to study these effects on crime to understand the current state of the art and to determine if further research is needed before considering the criminogenic impacts of smart urban elements on crime.

Second, while there is a substantial literature on crimes in physical and cyber places, there appears to be limited information on the impact of integrated physical and digital elements operating together in connected places (rather than individual cybersecurity postures of systems) with shared responsibilities across multiple organizations. Research on crime patterns and security interventions needs to take a holistic approach to analyse the collective criminogenic impacts within connected places where smart infrastructures' cyberspaces interact with physical places with the potential to cause cascading impacts. Fast-paced advanced and emerging technological innovations are continuously changing the security threats that people, organizations, Governments, and the global economy as a whole face and the way we respond to these threats (Furfaro et al., 2023; Hudson-Smith et al., 2021; Vermesan et al., 2020). New technology, innovation and connected smart infrastructure are not just changing the cybercrime landscape, methods of committing crime and the ease with which crime can be committed, they are also creating new crimes altogether. Understanding the relationship between new urban elements seen in connected places and crime not only provides an interdisciplinary perspective for crime policy research, it also offers new ideas for creating safe and sustainable cities. Comprehensive research is needed on opportunities, threats, vulnerabilities, the effectiveness of security interventions, accountabilities and governance challenges in connected places to mitigate the security risks that may emerge in smart urban built environments.

Third, Environmental criminology approaches were developed to explain crime patterns in physical urban spaces, and these theories have been considered to explain crime in cyberspaces. However, digital spaces have inherently different features from physical spaces and hence researchers need to think how environmental criminology principles can be adapted for digital spaces and the changing smart environments

where urban infrastructure services operate concurrently in physical as well as cyber places.

To complement the findings from this chapter and meet the aims of this thesis, in the next Chapter, the existing empirical literature is explored more thoroughly using a systematic literature review to understand the quantitative effects of physical and cyber elements of the urban environment on crime.

Chapter Three

3 Study of physical crime patterns within the built environment

The aim of this chapter was to review the empirical evidence to collate what we know about the criminogenic features of the urban elements that are associated with physical crimes in the built environment. It was completed at the beginning of the PhD and was intended to inform the direction of the research that followed it. Research on crime and place consistently suggests that the spatial distribution of crime is strongly concentrated at local geographical levels i.e. small groups of 'micro' places and that these concentrations of crime events are stable over time (Groff, Weisburd, & Yang, 2010; Weisburd, Bernasco, & Bruinsma, 2009). For this reason, it is important to analyze factors that influence crime patterns at the micro level. Also important is the need to analyze the quantitative strength of any associations identified, as this can help to inform the design of appropriate security interventions (Groff et al., 2010). Not all studies of spatial patterns of crime conduct analyses at the local level, however, studies that examine patterns for larger macro places (such as census groups, census tracts or the neighborhood level) are likely to dilute estimates of the influence of features of the urban environment. Hence, the focus of this chapter was to understand research concerned with the influence of urban elements on crime in micro places. The overarching research questions were "Which urban elements have been quantitatively analyzed for their influence on physical crime using micro spatial units, and what is their estimated overall effect on crime?"

Different approaches to reviewing literature exist. While useful, ad-hoc or standard literature reviews are known to lead to the identification of biased samples of studies (Shuster, 2011). As such, two different reviewers conducting the same search may come to different conclusions. For this reason, Systematic Reviews (SRs) have emerged as a method of synthesizing evidence in a reproducible and unbiased way (Higgins et al., 2019). A SR methodology was thus used in this chapter. Studies were included in the SR if they examined patterns at micro places such as street segments, census blocks, individual addresses, or small clusters of these units.

To understand the criminogenic impacts more precisely, it was necessary to synthesise findings regarding the strength of any associations observed. Meta-analysis is a statistical tool for data synthesis which aims to obtain a single summary estimate of the combined effect size from multiple studies (Michael et al., 2011). Where possible, in what follows, a meta-analysis of the effect sizes of the association between urban elements and crime was conducted. This chapter starts with the study design for the systematic literature review (Section 3.1). Section 3.2 details the search results, and Section 3.3 presents the findings from a meta-analysis of the data extracted from the identified studies, with a discussion of overall findings presented in Section 3.4. and conclusion in Section 3.5.

3.1 Study Design

3.1.1 Search Strategy

The search strategy involved the use of combinations of keywords to find studies that met the study inclusion criteria (see below). In addition to searching for traditional features of urban environments, consideration was given to rapid advancements in technology in urban cities. For example, drones and public wifi can be used to conduct, prevent and detect crimes (Blythe & Johnson, 2021). Geographic information systems, computer simulations, social media and technology such as Artificial Intelligence (AI) and machine learning have been used to analyse influence of urban elements on physical crime patterns (Corso & Monday, 2015; Liu & Eck, 2008). The search keywords included these terms to ensure that research that quantitatively analyses correlation between urban elements and physical crimes using technology was searched.

Databases for online search

The databases searched were chosen to ensure that studies published in the outlets of a wide range of disciplines (e.g. criminology, urban planning, transport, social sciences, criminal justice, policing, and Government policies) would be identified. The databases identified were:

1. **ProQuest:** a multidisciplinary database that covers Australian Education Index , Avery Index to Architectural Periodicals, Digital National Security Archive (39 databases) , EBook central, Humanities Index, ProQuest Central (61 databases) and Social Science Premium collection (17 databases) (Proquest LLC., 2020).

2. **SCOPUS**: one of the largest and most prestigious databases for peer-reviewed literature which covers multi-disciplinary globally sourced articles from fields such as Science, Technology, Medicine, Social sciences, and Arts and humanities (Elsevier B.V., 2020b).
3. **Geobase**: a database that allows access to international geoscience literature that covers 2,772,739 abstract records (Elsevier B.V., 2020a).
4. **JSTOR**: a database that allows access to “12 million journal articles, books, images, and primary sources in 75 disciplines” (Ithaka, 2020).
5. **Campbell collaboration**: a leading source of world-wide research literature that informs policy makers (Campbell Collaboration, 2020).

Search terms

The above databases were searched using search strings formed as follows:

1. ProQuest Central, Scopus and GeoBase

The thematic keywords were divided into four search filters, as follows:

- a) **Filter A: Elements of street Design and urban planning** – Thematic keywords within this filter relate to physical urban environments, the design of the built environment, street characteristics, smart city elements and land use.
- b) **Filter B: Crime patterns and impacts** – Thematic keywords within this filter relate to crime analysis, and changes to crime.
- c) **Filter C: Crime types** – Thematic keywords within this filter relate to possible physical crimes that occur in the built environment.
- d) **Filter D: Quantitative analysis** - Thematic keywords within this filter are used to exclude studies that used only qualitative analyses or did not report any analyses.

Keywords for each of the above filters were identified through an initial scoping of the literature. The full set of keywords can be found in Appendix 1. Initially, searches conducted using generic keywords identified irrelevant results. For example, using street, crime, correlation, and design as separate keywords identified irrelevant studies such as the impact of one-way street design on collisions and studies on the sociological implications of crime. Hence, keywords were refined to be more specific. For example, by using the keyword “street” in the same sentence as “design”, and “crime” in same sentence as “deter*” within 5 words of

each other made the search more specific. The database searches examined words in the title, abstracts, and keywords of the studies. Keywords were combined using Boolean operators. For example, the search string for Filter A was created by connecting all the keywords using the logical operator “OR” (See Appendix 1–1), this was repeated for filters B, C and D (See Appendix 1– 2,3,4).

To find studies that contained keywords from more than one type of filter, the individual search results from each filter were combined using the Boolean AND operator. Searches were carried out with and without crime types (Filter C) as pilot testing suggested that a few studies that have analyzed the influence of urban elements on crime had not specified the crime type examined in the abstract or keywords. Thus, the results were derived from:

(Search results of Filter A AND search results of Filter B AND search results of Filter C AND search results of Filter D) OR (search results of Filter A AND search results of Filter B AND search results of Filter D).

2. **JSTOR:** This database has the limitation that search strings can only have up to 200 characters. Hence, after initial tests, specific keywords that best represented the scope of the review were identified. The Keywords were divided into three filters:

- a) Filter A: land use, built environment, micro place, street network, street configuration.
- b) Filter B: quantitative analyses, regression, correlation
- c) Filter C: crime pattern

The keywords for each filter are joined by the Boolean operator ‘OR’. The keywords across filters are connected through the Boolean Operator “AND”.

JSTOR Search string: (“land use” OR "built environment" OR "micro place" OR "street network" OR "street configuration") AND ("quantitative analysis" OR regression OR correlation) AND (criminogenic OR "crime pattern")

3. **Campbell Collaboration:** This database has 177 records only. So, the database studies were searched manually.

Identification of Data sources from the Grey Literature and Hand searches

Reports published by relevant organizations (see below) were identified and hand searched. Reports from these organizations were included in the review if they met the study inclusion criteria (See Section 3.1.2). The following were searched:

1. **Reports from relevant organizations in the UK:** Reports and websites from the following organizations were hand searched: The Home office, Transport for London, the UK College of Policing, the Office for the Deputy Prime Minister (ODPM), the Department of the Environment, Transport and the Regions, the Ministry of Housing and Communities & Local Government.
2. **Reports from relevant organizations in the US:** Reports and websites of the following organizations were hand searched: the National Institute of Justice, The Police Foundation and the Department of Homeland security.
3. **Reports from relevant organizations in Australia:** Reports and websites of the following organization were hand searched: the Australian Institute of Criminology and the Australian Urban Design Research Centre
4. **Reports from relevant organizations in New Zealand:** Reports and websites of the following organization were hand searched: the Ministry for the Environment, and the Ministry for Justice
5. **Other:** The following were also hand searched: Research*eu magazine, United Nations Interregional Crime and Justice Research Institute (UNICRI) publications, and International CPTED Association (ICA) – CPTED Journal publications.

An academic librarian was consulted about the databases searched and the formulation of the search strategy. A systematic review protocol, which detailed the method used here and was produced before the searches were conducted, was peer reviewed by two independent researchers. The key feedback provided was to use variations of spellings for keywords, for example usage of “neighborhood” and “neighbourhood”. The search criteria were adjusted based on these recommendations.

Identification of Data sources from Forward and Backward searches

Forward searches were conducted by identifying key (highly cited) studies and looking for studies that cited them. Backward searches involved identifying studies (in those studies identified through the above searches) that were “cited” as providing empirical

findings relevant to the review. Studies identified through forward or backward searches were included if they met the inclusion criteria.

3.1.2 Criteria for inclusion and exclusion

The following initial eligibility criteria were used to decide whether to select or exclude studies:

1. Studies must be from a credible source or peer reviewed and in English: All peer-reviewed academic papers and conference proceedings were included. Grey literature, such as organizational reports, were included if they were authored by a credible source. This included, for example, Transport for London (UK) and the Home Office. Magazine studies (except for Research*eu magazine mentioned in section 3.1.1) and online blogs were not included as these are not credible sources for quantitative analysis and are rarely subjected to quality assurance (such as peer review). Research studies not written in English were excluded as translating text written in foreign languages was beyond the scope of this review.

2. Studies must focus on urban areas and discuss the influence of specific urban design elements on crime patterns: Studies that focused on urban areas such as cities, towns and suburbs were included in the review. Studies that examined crime for areas that lack typical urban characteristics were excluded. For example, a study conducted on a self-contained university campus did not meet the inclusion criteria, but one conducted in a university town (e.g., Cambridge and Oxford in the UK), met the inclusion criteria. Only the main effect of a specific urban element on crime was included. For land uses to be included in the SR, the study needed to describe what urban element(s) was being analysed specific to that land use. For example, retail land use might include grocery stores, cafes as described in Bowers (2014).

Studies included in the systematic review must use predictor variables, also known as independent variables, to estimate the impacts of physical urban elements on (or associations with) one or more crime types. Studies that did not clearly define the predictor variables were excluded. For example, predictor variables such as generic recreational uses of land (rather than a leisure facility), a specific type of housing, drug markets which can shift in urban places dynamically, and generic Government buildings were excluded.

Studies that used predictor variables that did not measure the main effect of an urban element on crime were excluded. For example, studies that examined the interaction/ combined effects of multiple urban elements (e.g. public transit stop close to a park situated on a main street) on crime (but not the unique effect of each element) were excluded. Studies that examined specific temporal effects alone, such as a criminogenic facility opening for additional hours were excluded, unless they also examined the effect of the facility in general. Also excluded were studies that examined only spatial lag effects, such as examining the effect of an urban element on neighboring areas but not the area within which the urban element was located. Similarly, studies that focused on the internal characteristics of urban elements (such as the internal design of a station/building) were also excluded from SR. For example, influences on crime due to an underground rail station and the street network surrounding it met the inclusion criteria, however, the analyses of crime within an underground station must be excluded.

Studies that did not examine associations between urban design and crime but focused on other “area level” factors were excluded from the review. For example, studies that considered social factors, perceptions, or fear of crime were excluded unless they also considered the correlation between elements of urban design and crime.

3. Studies must analyze crime patterns quantitatively: Studies for which the influence on crime of features of the urban environment were measured quantitatively were included. Studies which did not collect any empirical data, were excluded. As qualitative studies do not explicitly measure associations, they were excluded from this review.

4. Studies must analyze crime patterns based on credible and precise sources of data: Studies that used data that lacked spatial accuracy were excluded. For example, data directly provided by police departments (which is usually accurate to a resolution of one metre, or similar) were included, but data provided by (for example) police.uk and public websites were excluded as these data are known to be (spatially) inaccurate (Tompson et al., 2014).

5. Studies must not analyze crime patterns using data from the Covid-19 pandemic period – 2020 to 2022: Studies that used data from the period when the Covid pandemic struck were excluded as crime patterns were very different to other

periods of time due to the “stay at home” mandates imposed on people by Governments world-wide (Abrams, 2021; Díaz et al., 2022; Zhang & Chen, 2023).

6. Studies must have conducted quantitative analysis using micro spatial units:

For a study to be included, the authors had to clearly define the spatial units employed and these had to be small. The reason for the latter is that – as discussed in section 3.1.1 – research (Weisburd, 2015; Groff, Weisburd, & Yang, 2010; Weisburd, Bernasco, & Bruinsma, 2009) suggests that crime is highly concentrated at the 'micro' level of place and the factors that influence crime are likely to operate at this level. As such, estimates of the influence on crime of features of the urban environment may be diluted if they are studied using large spatial units. Studies that used smaller spatial units, such as street segments, 400-500 feet buffer zones around a place (the average length of a street block), or 500ft² grid cells were included. Block faces are the smallest units of Census geography in the USA (Roberto, 2018), and so the decision was taken to include studies that used this unit of spatial analysis. Studies that did not define the spatial unit of analysis employed or had a very large spatial unit, such as census tracts, dissemination areas (which are often used in Canada) or large neighbourhoods were excluded.

3.1.3 Approach to Meta-analysis

There are two common approaches to synthesizing findings from quantitative studies. The first approach is called vote-counting and is often used where estimates of effect size cannot be combined to compute an overall effect size estimate, but where the direction and significance of the results can be interpreted to understand the overall direction of the effect (Bushman, Brad, & Wang, 2009). This approach divides the studies into two stacks - statistically significant results that provide evidence in favor of the hypothesis and non-significant results that do not. It is concluded that there is no effect if the number of studies in the latter is higher than those in the other stack. Alternatively, if more studies suggest an effect, conclusion is drawn in favor of the hypothesis (Friedman, 2001). The second approach is statistical meta-analysis. Here, weights are assigned to the estimates reported in each study before they are combined to calculate both an overall effect size and a standard error that is associated with it. The weights applied account for the reliability of each study estimate. This produces a weighted estimate that describes the overall size and direction of the effect to be estimated (Braga et al., 2014; Michael et al., 2011). By

combining the findings of two or more studies in this way, a meta-analysis provides more statistical power (i.e. smaller standard error of the weighted average effect size than the findings from a single study), whilst also increasing the precision (i.e. smaller confidence interval) of the summary effect size (Johnson et al., 2014; Cohn & Decker, 2003; Lipsey & Wilson, 1961; Neyeloff, Fuchs, & Moreira, 2012). Where there are sufficient data, meta-analysis also enables the investigation of variation across studies to see what factors might explain this.

3.1.4 Grouping data for meta-analysis

To visualize the findings that follow, Forest plots are used to show the individual effects from each study as well as the overall mean effect for similar studies. The studies that met the inclusion criteria were grouped based on the type of crime and predictor variables used. When there was only one study in the group, meta-analysis could not be conducted. However, the data for each study is shown on the Forest plot. Research on Situational Crime Prevention (SCP) suggests that situational factors influence different crime types in different ways making it important to analyse crime patterns separately for each crime type (Beavon et al., 1994; Brantingham & Brantingham, 2013; Curman et al., 2015; Groff et al., 2010; Weisburd et al., 2012). This approach was taken here, and analyses were reported separately for property, violence, disorder, and drug crimes.

3.1.5 Methodology for meta-analysis

Studies usually estimate effect sizes using statistical regression models of one kind or another. Where possible, Effect Sizes (ES) and Standard Errors (SE) were extracted from the included studies. Different statistics reported by study authors could include an Incident Rate Ratio (IRR) or a raw regression coefficient. Hence, to combine effect sizes for the meta-analysis, it was necessary to convert them to a common metric. Here, IRRs were converted to coefficients using the following formulae:

$$\text{Coefficient value} = \ln(\text{IRR})$$

Where the precision of the estimates (i.e., the standard errors) were not directly reported in a study, the approach to estimating them varied according to what data were reported and which type of test statistic was available. The SE of the coefficients

were calculated (Kulinskaya, Morgenthaler, & Staudte, 2007 ; Lipsey & Wilson, 1961) using the standard formula:

$$SE\ of\ coefficient = \frac{Coefficient\ value}{z}$$

Where a z value was not provided, the z value was estimated using the p-value reported (Kulinskaya et al., 2007; Lipsey & Wilson, 1961). Where an exact p-value was not provided, the highest value of p based on the significance level indicated was assumed (For example, for $p < 0.01$, a value of $p = 0.009$ was taken). This approach is not perfect but represents the most justifiable one.

Where the SE of a coefficient was not provided, but an IRR and the SE of the IRR was provided, the SE of the coefficient was estimated (Kulinskaya et al., 2007; Lipsey & Wilson, 1961) using the formula:

$$SE\ of\ Coefficient = SQRT\left(\frac{SE\ of\ IRR^2}{IRR^2}\right)$$

The 95% Confidence Interval (CI), Lower Confidence Interval (LCI) and Upper Confidence Interval (UCI) were calculated (Kulinskaya et al., 2007; Lipsey & Wilson, 1961) using the standard formulae:

$$CI = 1.96 * SE$$

$$LCI = ES - CI$$

$$UCI = ES + CI$$

Two approaches can be used to compute combined effect sizes across multiple studies – the fixed effects and random effects models (Lipsey & Wilson, 1961). The fixed-effects model assumes that the true effect size is the same across the entire population of studies, and any variance is caused only by random inherent errors (Lee et al., 2016; Lipsey & Wilson, 1961). The summary effect in a fixed-effects model is our estimate of this true effect size. A random-effects model assumes that the true effect size varies across the population of studies and the studies in the analysis represent a random sample of these effect sizes (Lee et al., 2016; Lipsey & Wilson, 1961). The summary effect size is the estimation of the mean of a distribution of these effect sizes

(Borenstein et al., 2010). In a meta-analysis, effect sizes are weighted by study prior to estimating the combined effect size. This is done in such a way that those studies with more precise estimates are given more importance. So, large studies with smaller variance contribute more to the weighted average combined effect size. As the random-effects model assumes that the effect can vary across studies, the weighted average combined effect size is computed using between-study as well as within-study variance. This gives a more conservative estimate of the overall effect size, and a larger overall standard error, compared to the fixed-effect model (Lee et al., 2016; Lipsey & Wilson, 1961). This estimate is likely to be less biased and more accurate than the fixed-effect alternative. Hence, I use a random-effects model for meta-analysis here.

Various methods are available to estimate the weights of the studies included in a meta-analysis (Helfenstein, 2002). For a random-effects model, the weights are inversely related to the total variance. Estimators that produce iterative estimates of between-study variance include the restricted maximum likelihood (REML), maximum likelihood (ML) and empirical Bayes (EB) methods. There is insufficient research that evaluates EB. REML is suited to analysis that involves many studies or where the variance between studies is large; in contrast, ML is better suited to analyses that involve small amounts of variance between studies (Kulinskaya et al., 2007). The effect size and standard error variance for the studies analysed were generally low. Hence, the meta-analysis was conducted using a random effects model and the ML estimation method. All values were computed using the meta commands in STATA/MP 16.0 for windows using the following commands:

```
meta set ES SE  
meta summarize, random(ml)
```

The outputs from the above commands also indicated whether the heterogeneity between the individual studies was significant. Finally, for each analysis, the exponential value of the combined ES was calculated to convert it to a standard measure of IRR. LCIs and UCIs were computed across studies within each group and displayed in a forest plot.

3.2 Search Results

Searches were conducted in January 2020 using the identified query strings, forward searches, backward searches, and a review of the grey literature. A further search was conducted to include studies published between February 2020 to August 2024.

3.2.1 Screening of search results

The search results were screened in two phases – in January 2020 and August 2024. The collective search results yielded 721 studies, while 7 other studies were extracted manually resulting in a total of 728 studies. These were imported into the web-based tool Covidence (www.covidence.org) and (224) duplicate studies were automatically removed. Following further manual screening, 6 more studies were manually identified as duplicates. Consequently, a total of 230 studies were marked as duplicates and 498 studies were screened further (see Figure 3-1). Of the 498 studies screened, 323 were marked irrelevant based on Title and Abstract, as they discussed non-urban entities, crimes that were out of scope (e.g., fraud) or did not conduct a quantitative analysis of the impact of urban elements on crime. Full text screening of the remaining 175 studies resulted in the removal of 81 studies (94 studies remained). Of those that were removed:

- a) 21 study were not written in English (although the abstract was).
- b) 15 studies that did not use a credible data source, crime data was downloaded from public websites rather than from police departments,
- c) 27 studies did not assess the influence of urban elements on crime or did not assess these quantitatively,
- d) 3 studies assessed crimes associated with the internal features of urban elements,
- e) 14 studies included data from Covid-19 pandemic period
- f) 1 study discussed specific scenarios such as dissident Republican violence in Belfast

From the 94 studies that remained, 65 studies were excluded as they used large spatial units. Five of these did not define the spatial unit of analysis (one of which was a systematic literature review that assessed various models that measured the spatial effect of alcohol consumption on crime). The purpose of the meta-analysis reported here was to estimate the strength of the effect of the independent variables

on crime across multiple studies and not the trends over a period, hence, one study that used such percentage changes in trends without providing the actual effect size was also excluded. Ultimately, 29 studies that used micro spatial units were included in this review.

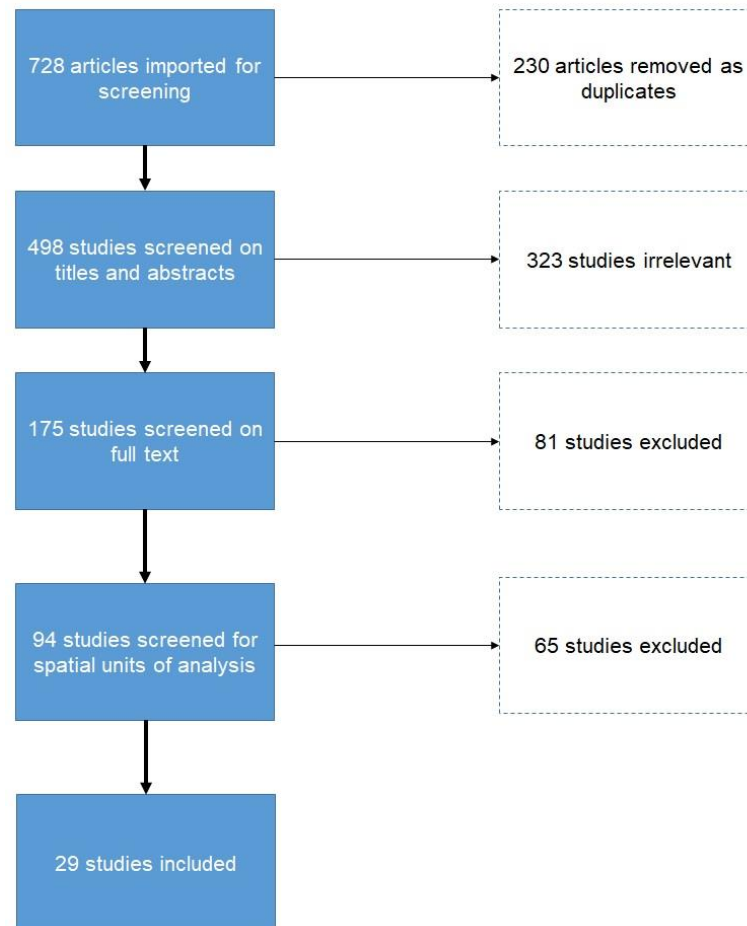


Figure 3-1 Prisma Chart of search process for systematic review

To assess Inter-rater reliability, two reviewers screened the titles and abstracts of 20% of the studies, applying the inclusion criteria described above. IRR i.e. the degree of agreement among peer reviewers was assessed based on two parameters, inclusion and exclusion (Virta, 2013). The Prevalence-Adjusted Bias-Adjusted Kappa (PABAK) statistic was computed to determine how consistent the ratings were. The kappa values can be interpreted as: <0.4 indicates agreement level not fit for purpose, 0.40–0.59 indicates fair agreement, 0.60–0.74 indicates good agreement and >0.75 indicates high agreement (Tang et al., 2011). The PABAK measure of 0.78 indicated that there was high agreement between the reviewers, and consequently one reviewer screened the remainder of the studies.

3.2.2 Data Extraction

A spreadsheet was used to manually extract information from the articles that met the inclusion criteria. A pilot exercise was completed for a sample of articles to ensure that data was captured in a reliable manner. The following details were extracted from articles that met the eligibility criteria:

- Title of the article
- Authors
- Year of study
- Brief description of the study
- Type of publication (e.g., journal, grey literature)
- City and country where the study was conducted
- Urban element (e.g., trees, bicycle parking, bus stop)
- Crime type examined (e.g., antisocial behaviour, burglary)
- Data sources and time-period
- Spatial unit of analysis
- Study design (e.g. longitudinal study, cross sectional study)
- Type of the statistic and statistical model used to examine association between crime and street element (e.g., Regression coefficient, bivariate correlation, hierarchical linear models, single level models)
- Type of study design (cross sectional, time series, experiment)
- Description of quantitative result (e.g. associated findings, context specific dependencies)
- Correlation of urban Street element with crime as found in the study (e.g., bus stop increases crime, decreases crime, or has no impact)
- Statistic value and precision (number)
- Comment (e.g., any additional findings, constraints of the model)

The extracted data from 29 studies that met the inclusion criteria are listed in Appendix-2.

3.2.3 Characteristics of included studies

Studies included in the SR were conducted across eight countries –Brazil, Canada, China, Israel, Italy, Mexico, UK, and USA. The urban elements (40) that were defined and assessed in the included studies are listed in Table 3.1.

Table 3.1 Urban Elements found in studies included in SR

Urban elements	Number of assessments	Studies
Street Network, Configuration and other features	12	(Bernasco & Block, 2011), (Clutter et al., 2019), (Davies & Johnson, 2015), (Groff & Lockwood, 2014), (Vilalta & Fondevila, 2019), (Beavon et al., 1994), (Johnson & Bowers, 2010), (Summers & Johnson, 2017), (Kim & Hipp, 2019), (Kim & Wo, 2023), (Favarin, 2018), (Xie et al., 2022)
Public Transit	10	(Bernasco & Block, 2011), (Hsu & Miller, 2017), (Clutter et al., 2019), (Amram et al., 2024), (Soohyun & Yongjei, 2016), (Favarin, 2018), (Liggett et al., 2003), (Groff & Lockwood, 2014), (Haberman & Ratcliffe, 2015), (Newton et al., 2014)
Retail land use	11	(Bowers, 2014), (Clutter et al., 2019), (Soohyun & Yongjei, 2016), (De Souza & Miller, 2012), (Favarin, 2018), (Haberman & Ratcliffe, 2015), (Kim & Hipp, 2019), (Kim & Wo, 2022), (Bernasco & Block, 2011), (Hsu & Miller, 2017), (Vilalta & Fondevila, 2019),
Alcohol outlets	10	(Bernasco & Block, 2011), (Clutter et al., 2019), (Favarin, 2018), (Groff & Lockwood, 2014), (Haberman & Ratcliffe, 2015), (Vilalta & Fondevila, 2019), (Liggett et al., 2003), (Groff, 2014), (De Souza & Miller, 2012), (Ratcliffe, 2012)
Schools	7	(Clutter et al., 2019), (Soohyun & Yongjei, 2016), (Favarin, 2018), (Groff & Lockwood, 2014), (Haberman & Ratcliffe, 2015), (Wo & Park, 2020), (Kim & Wo, 2022)
Parks	5	(Groff & Mccord, 2012), (Haberman & Ratcliffe, 2015), (Clutter et al., 2019), (Hsu & Miller, 2017), (Boessen et al., 2018)
Drug treatment centers	3	(Clutter et al., 2019), (Groff & Lockwood, 2014), (Haberman & Ratcliffe, 2015)
Bank branches and ATM	2	(Favarin, 2018), (Haberman & Ratcliffe, 2015a)
Hotels	2	(Clutter et al., 2019), (Kim & Wo, 2022)
Shopping malls	2	(Kim & Wo, 2022), (Vilalta & Fondevila, 2019)
Alley ways and windows onto street	2	(Beavon et al., 1994), (De Souza & Miller, 2012)
Trees	2	(Deng, 2015), (Xie et al., 2022)
Walkability	2	(Lee & Contreras, 2021), (Xie et al., 2022)
Police stations. Total units of public housing on each street segment	1	(Favarin, 2018)
Public libraries, recreation centers	1	(Clutter et al., 2019)
Abandoned buildings, vacant land, mailboxes, parking lots, Churches	1	(Hsu & Miller, 2017)
Halfway houses	1	(Groff & Lockwood, 2014)
Fire stations	1	(Ratcliffe, 2012)
road density in the areas surrounding the street segments, walkability, the proportion of grass in the streetscape, the greening rate and the number of - streetlamps, sidewalks, enclosure effects, fences, number of buildings in street scape, number of walls in streetscape and number of trees in streetscape	1	(Xie et al., 2022)
Physical boundaries between two sides of streets (Land use difference)	1	(Y.-A. Kim & Hipp, 2022)
Number of businesses, Percentage of buildings built in past 10 years, community center and educational building within 500m of center of street segment, garden within 150m of street segment	1	(Amram et al., 2024)

With respect to study design, two studies employed matched case-control design, whereas the remaining 27 studies were cross sectional studies. None of the studies used Randomized controlled trial (RCT) which involves a scientific experiment and is more reliable method of assessment. Studies mainly included analyses of urban elements on violent crimes, property crimes, disorder crimes, and drug crimes using Negative Binomial or similar regression models (see Table 3.2). The studies provided correlation of predictor variables associated with features of urban elements with crime. A correlation is a statistical measure that describes the extent to which two

variables are related. While correlation can provide valuable insights into the relationships between variables, it does not imply causation. Causation means a change in the first variable directly leads to a change in the second. However, correlation describes relation between predictor variables and crime, it does not state that crime is a result of the predictor variable.

Table 3.2 Statistical models used by studies in SR

Statistical models used	Number of studies N=29
Negative Binomial or equivalent Regression models	16
Zero-inflated Negative Binomial (ZINB) model	3
ANOVA or equivalent model	2
Poisson Hierarchical Linear Model	2
Conditional Logistic Regression Model	2
Ordinary Least Square (OLS) fixed effect Linear Regression model	1
Multivariate Least Square (OLS) Regression model	1
Multivariate Linear Regression Analysis	1
Machine learning model	1

The spatial units of analysis used in the studies mainly included census blocks, street segments, 50x50 m grid cells, 500- ft² grid cells, and buffer area² (distance in feet/ meters) around the urban elements as seen in Appendix 2. Studies that used the census block as the unit of analysis were included as this was the smallest spatial unit used in the studies conducted in the USA.

Only one included study by Xie et al. (2022) analysed the association between crimes with locations using digital applications based on a machine learning model. To validate the search strategy which expected studies where cyber activities of people analysed for association with physical crimes were to be included, a sample of 25% of the rejected studies were reviewed. As seen in Section 3.2.1, 65 studies were excluded as they used large spatial units, and 27 studies were excluded as they either did not assess the influence of urban elements on crime or did not assess these quantitatively. Out of these 92 studies, 25% of studies selected by a random sampling method fetched 23 studies. It was found that six of these studies specified algorithms for crime prediction in smart cities using Data mining machine learning models, geographic information systems and crowdsourced data. Examples include studies related to i) geographic patterns of assaults, burglaries, and robberies using Facebook

² Note: the number of facilities were regressed from each grid cell/ buffer area

data pertaining to people's interests within a zip code (Fatehkia et al., 2019), ii) big data analysis to understand patterns of crime in urban environments by associating 911 calls with gunshot detection sensors (Renda & Zhang, 2019), iii) effect of Streetscape Environment on Crime Using google Street View Images (Deng et al., 2021), iv) spatiotemporal impacts of people's geotagged tweets on crimes such as assault, burglary, robbery, and theft at neighbourhood level (Bendler et al., 2014; Liu et al., 2020), v) spatial association of tweets on social media data with acquisitive crimes in London (Wang & Li, 2022), and vi) the correlation between bicycle theft in Beijing and online searches carried out by people (Ding et al., 2019). These studies used digital data analysis techniques or assessed the cyber activities of people that could impact physical crimes; however, the data analysis was conducted using larger spatial units. This could be due to the nature of the large urban data sets. Hence, although these studies were relevant to the scope of this SR, they did not meet the inclusion criteria.

3.3 Meta-analysis

The data for the 29 studies that met the inclusion criteria were assessed to determine suitability for meta-analysis. Meta-analysis is appropriate only when the interpretation and combination of data from two or more studies would be meaningful. Many of the studies identified in the systematic review used data collected for different spatial units of analysis and different predictor variables. If studies are very heterogeneous in terms of what they measure and how they do so, it may be inappropriate to attempt a statistical meta-analysis since this would involve combining data that are not comparable. Hence, to analyze the relationship between the urban elements considered and crime, it was important to assess whether the data could be combined in a meaningful way.

Meta-analysis in the sub-sections that follow, was conducted where a) statistical models were comparable b) a point estimate of the effect size associated with a feature of the environment was reported with a measure of precision, or parameters that would enable precision to be estimated (e.g., a t-statistic, or p-value). There were eight urban elements for which suitable effect sizes and standard errors were available. Where data were suitable, a statistical meta-analysis was conducted, and effects were summarised in a Forest plot. For some combinations of urban elements and crime types there was insufficient data to perform a statistical meta-

analysis. Rather than exclude this data, the effect sizes were also plotted to provide the reader with a graphical representation of the effect size and direction and to enable them to “triangulate” the data. Taken together, the plots assess the strength (and consistency) of the best available evidence as to which features of the built environment appear to influence crime and how they do so.

3.3.1 Street Network, Configuration and other features

Twelve studies (discussed below) assessed the impact of types of street layout, networks, connectivity, and permeability on crime (see Table 3.3). All studies showed consistent results - positive correlation between property & violent crimes and street accessibility.

Three studies (Bernasco & Block, 2011; Groff & Lockwood, 2014; Vilalta & Fondevila, 2019) analysed the effect of main roads on crime, all finding a positive association. Groff & Lockwood (2014) found that major roads (expressways, major arterials, and minor arterials) were significantly related to counts of violent, property crime and disorder. This study was conducted in Philadelphia, USA using street segments as the unit of analysis (Groff & Lockwood, 2014). Groff & Lockwood (2014) studied the influence of major roads on crimes for up to distances of 400, 800 and 1200 feet away; of which 400 feet was included in meta-analysis as it is a smaller unit. Vilalta & Fondevila (2019) studied crime risks in the Santa Fe neighbourhood, Mexico City, Mexico and found that there was a high positive correlation of crimes in a block on the main avenue compared to the blocks on smaller streets (Vilalta & Fondevila, 2019). Bernasco & Block (2011) studied robberies in Chicago, USA. They concluded that blocks that include crime attractors and generators have a high risk of robbery, and this risk increased when the block was along the main road (Wim Bernasco & Block, 2011).

Beavon et al. (1994) studied property crimes (incident of bicycle theft, auto theft, theft from auto, burglary, wilful damage, break and enter, other property theft) in Maple Ridge and Pitt Meadows, British Columbia. The study used street segments as the unit of analysis and found crime risk to be higher on accessible street segments (those with more connections) (Beavon et al., 1994). However, Beavon et al. (1994) did not provide effect size and precision, and hence this study was excluded from the meta-analysis. Johnson & Bowers (2010) conducted a study in Merseyside, UK to analyse

Table 3.3 Influence of Street Configuration on crime - Assessment of studies for inclusion in meta-analysis

Authors and Year of Study	Crimes studied in Urban Area	Study Design	Predictor variable and correlation with crimes	Spatial unit of analysis	Effect size and Precision	Statistical model	Include in meta-analysis
Johnson & Bowers (2010)	Burglary (Property) crime in Merseyside, UK	Cross sectional study	Major roads correlated positively and significantly	Street segment	Provided	Poisson Hierarchical Linear Model	Y
Groff & Lockwood (2014)	Property, violent and disorder crimes in Philadelphia, USA	Cross sectional study	Distance of facility from street segment (400, 800, 1200 ft) correlated positively	Street segment	Provided	Negative Binomial regression model	Y
Bernasco & Block (2011)	Robbery (Violent crimes) in Chicago, USA	Cross sectional study	Any main street along block correlated positively (significant)	Street segment	Provided	Negative Binomial Regression Models	Y
Vilalta & Fondevila (2019)	Violent crimes in Santa Fe, Mexico city, Mexico	Cross sectional study	Main Avenue correlated positively	census block	Provided	Geographically weighted Poisson regression model	Y
Clutter et al. (2019)	Street robbery (Violent crimes) in Business Improvement District (BID) of Cincinnati, USA	Cross sectional study	Betweenness correlated positively	Street blocks (segments)	Provided	Negative Binomial regression model	Y
Summers & Johnson (2017)	Violent crimes in UK	Cross sectional study	Connectivity Accessibility, Global choice (R=3000 m) Betweenness correlated positively	Street segment	Provided	Zero-inflated Negative Binomial (ZINB)	Y
Davies & Johnson (2015)	Burglary (Property) crime in Birmingham, UK	Cross sectional study	Betweenness, Permeability (3000m) correlated positively (significant)	Street segment	Provided	Poisson Hierarchical Linear Model	Y
Kim & Hipp (2019)	Burglary (Property) crime - Acquisitive crimes (and violence) in Southern California region, USA	Cross sectional study	Effect of 1/4 and 1-mile Betweenness – weighted by employees in Retail, service, restaurant, store correlated positively.	Street segment	Provided	Negative Binomial Regression model used non-linear (curvilinear) relationship between street activity and crime levels	N – what is measured using predictor variable betweenness is not comparable with other studies
Favarin (2018)	Property and violent crimes in Milan, Italy	Cross sectional study	Streets with limited access correlated negatively with burglary and association was insignificant with robbery	Street segment	Provided	Negative Binomial Regression model	N – 'streets with limited access' not defined, no clarity about what was measured
Beavon et al. (1994)	Property theft crimes in Canada	Cross sectional study	Accessibility measures - Flow and turns correlated positively	Street segment	Not provided	MANOVA	N – Did not provide effect size and precision
Kim & Wo (2023)	Aggravated assault, robbery (Violent) crimes; burglary, larceny, and motor vehicle theft (Property) crimes in San Francisco, USA	Cross sectional study	Elevation, slope, elevation differences generally correlated negatively, and street connectivity generally correlated positively across crimes	Street segment	Provided	Negative Binomial Regression model	Y
Xie et al. (2022)	Property crimes in ZG city, China	Cross sectional study	Street length, road density correlated positively	Street segment	Not provided (Provides effect size values from machine learning model)	Machine learning model	N – what is measured using predictor variable betweenness is not comparable with other studies
Total studies assessed –12, Studies included in meta-analysis –8, Studies excluded from meta-analysis - 4							

the influence of the accessibility of the street network on crime risk using street segments as the unit of analysis. They found that the risk of residential burglary was higher with increased accessibility, and when a street segment was classified as being part of a major road. The burglary risk for a permeable (i.e., accessible) street was higher when housing density was higher and ethnic heterogeneity was high. The risk of burglary was found to be lower on street segments classified as private roads and on cul-de-sacs (particularly those that were sinuous — or bendy — in nature) (Johnson & Bowers, 2010).

Summers & Johnson (2017) studied the influence of betweenness on serious violent crimes (i.e., crimes including homicides, attempted murders, and assaults) in one London borough (UK). Betweenness measures how frequently street segments feature in shortest paths i.e. how likely these street segments are used by people for their journeys through the street networks (Davies & Johnson, 2015). The measures of connectivity used by Summers & Johnson (2017) were local, as well as global for integration (to-movement potential) and choice (through movement potential). The risk of violence was found to be higher on roads with higher estimated to-movement and higher estimated through-movement, an effect which also spilled over to nearby segments (Summers & Johnson, 2017). It was also found that higher connectivity associated with higher pedestrian and vehicle movements, and correlated with lower crime incidence (Summers & Johnson, 2017).

Davies, & Johnson (2015) studied the influence of the configuration i.e. arrangement of street networks on burglary in Birmingham, UK using street segments as the unit of analysis. The study found that betweenness was co-related with counts of burglary. As with Johnson & Bowers (2010), burglary was negatively correlated with the linearity of streets – linearity arguably provides better visibility (Davies, & Johnson, 2015).

Kim & Wo (2023) studied the effect of physical land surface and network of street segments using four predictor variables (elevation, slope i.e. steepness, differences in elevation – i.e. hilliness and betweenness i.e. Connectivity - see Table 3.3) on robbery, aggravated assault, burglary, larceny, and Motor Vehicle Theft (MVT) in San Francisco, USA. Differences in elevation and betweenness were measured for surrounding $\frac{1}{4}$ mile. For property crimes, burglary correlated negatively with all the four predictor variables; MVT correlated negatively with elevation and slope (%) whereas MVT correlated positively with differences in elevation and betweenness;

Larceny correlated negatively and significantly with all predictor variables except betweenness which had positive correlation (Kim & Wo, 2023). For violent crimes, aggravated assault correlated positively with all predictor variables. Robbery correlated positively with elevation and betweenness; and correlated negatively with slope (%) and differences in elevation (Kim & Wo, 2023). It was found that the criminogenic effects of betweenness are “dampened by hilliness” in line with the least effort principle (Eck, Clarke, & Guerette, 2007) wherein offenders tend to choose locations/targets where least effort is involved (see Chapter 2, section 2.1). Potentially, this resulted in negative correlation of elevation and elevation differences with crimes (Kim & Wo, 2023). When the elevation difference is high, street segments with high betweenness have a robbery rate that is 16% larger in comparison to street segments with low betweenness (67% if elevation difference is low) (Kim & Wo, 2023). Although the slope (%) i.e. steepness is associated with lower rates of crime, the change in the criminogenic effect sizes on a street segment is low compared to other street typology measures (Kim & Wo, 2023). This could be because the slope can hinder the visibility of victims and offenders (Kim & Wo, 2023).

Favarin (2018) also used street segments as their unit of analysis in Milan, Italy and found that streets with limited access had lower levels of burglary crimes, whereas the effect was insignificant for robbery crimes (Favarin, 2018). Favarin (2018) examined crime concentration at the street segment level by examining streets with limited access in Milan-Italy, however, the authors did not provide a definition of what streets with limited access were and what was being measured, hence this study was excluded from meta-analysis. Xie et al. (2022) studied in XG city China, the effect of the number of pedestrians on street, street length, and road density on property crime and found a positive correlation (Xie et al., 2022). The study was carried out using machine learning models and SHAP (Shapley additive explanation) framework (Xie et al., 2022). This method of measuring the effect sizes was not comparable with other studies and hence this study was excluded from meta-analysis.

Clutter et al. (2019) analysed street segments in the Business Improvement District (BID) of Cincinnati, USA and found that betweenness was positively associated with higher counts of robbery. The robberies per foot on the street segments within the BID were found to be approximately double the number of robberies outside the business district. As the distance increased from the BID, the robbery risk on the street segment reduced by 3.5%. The study authors recommended

that future research should consider whether the features of street segments and not just the features of BID also contribute to rates of robbery (Clutter et al., 2019).

Kim & Hipp (2019) used betweenness centrality measures in Southern California, USA and assessed their association with violent and property crimes. They found that street segments that are more likely to be used (i.e., had higher betweenness) were associated with increased violent (aggravated assault, robbery) and property (burglary, motor theft, larceny) crimes; however, after reaching a threshold, property crime was found to decrease with increased betweenness at non-local distances (Kim & Hipp, 2019). As discussed earlier, the betweenness measure estimates how likely it is for a street to be used. The authors used weighted betweenness by population and the number of employees for four types of business (retail areas (more travellers), service, restaurants and stores) (Kim & Hipp, 2019). While this was fine, the quantitative analysis was completed using a non-linear model. Specifically, the authors included squared and cubic terms for the betweenness measures to examine the relationship between estimated street activity and crime levels. This represents a departure from the general approach taken in all other studies and makes it difficult to combine the data in a meaningful way and hence this study was excluded from meta-analysis.

3.3.1.1 Data synthesis

The data were divided into groups based on the predictor variables used and crime types examined in the studies analysed. All studies used a cross-sectional design that estimated levels of crime for a fixed period, but the studies varied in terms of how they measured the influence of the street network. As discussed, the crimes considered across studies also varied and included property crimes, violent crimes, and disorder. These are assessed separately here due to differences in their opportunity, and the nature of these offences. The crime of disorder includes conduct that may not be categorised as violent but nor is it comparable to property crimes. Kim & Wo (2023) provided main effects for three types of property crimes (burglary, larceny and motor vehicle theft) and two types of violent crimes (robbery, aggravated assault). The lowest and the highest main effects were included in meta-analysis for both crime types (providing best- and worst-case scenarios).

The grouping of the data is summarised in Table 3.4. Some studies appeared in more than one group as they reported findings for more than one crime type. The

data in the group with only one study (see Table 3.4) are not synthesised mathematically but the effect sizes are shown on the forest plot in the Results section.

Table 3.4 Data Analysis-Influence of Street Configuration on crime grouped by predictor variable and crime type

Authors and Year of Study	Included in Meta-analysis	Included in Forest plot
Property crimes		
Predictor variable Main Road – Property crimes (2 studies)		
Johnson & Bowers (2010)	Y	Y
Groff & Lockwood (2014)	Y	Y
Predictor variable Betweenness – Property crimes (2 studies)		
Davies & Johnson, (2015)	Y	Y
Kim & Wo (2023)	Y	Y
Predictor Variable (Street features) - Elevation – Property crimes (1 study)		
Kim & Wo (2023)	N	Y
Predictor Variable (Street features) - Slope – Property crimes (1 study)		
Kim & Wo (2023)	N	Y
Predictor Variable Differences in (Street features) - Elevation – Property crimes (1 study)		
Kim & Wo (2023)	N	Y
Violent crimes		
Predictor Variable Main Road– Violent crimes (3 studies)		
Groff & Lockwood (2014)	Y	Y
Bernasco & Block (2011)	Y	Y
Vilalta & Fondevila (2019)	Y	Y
Predictor Variable Betweenness – Violent crimes (3 studies)		
Clutter et al. (2019)	Y	Y
Summers & Johnson (2017)	Y	Y
Kim & Wo (2023)	Y	Y
Predictor Variable (Street features) - Elevation – Violent crimes (1 study)		
Kim & Wo (2023)	N	Y
Predictor Variable (Street features) - Slope – Violent crimes (1 study)		
Kim & Wo (2023)	N	Y
Predictor Variable (Street features) - Differences in Elevation – Violent crimes (1 study)		
Kim & Wo (2023)	N	Y
Disorder crimes		
Predictor variable Betweenness – Disorder crimes (1 study)		
Groff & Lockwood (2014)	N	Y

In the context of the street configuration and crime relationship, studies reported either incident rate ratios (IRRs), raw regression coefficients, or both to estimate the association between an individual independent variable (urban street configuration element such as accessibility to main roads) and the dependent variable (crime such as burglary). Relevant statistics (e.g., raw coefficient estimate, standard deviations of each variable in the model specification) from the tables, figures, or in the body of the text, were extracted from each study. Few studies provided a SE for the IRR or the raw coefficient while some did not provide an SE at all. For example, Clutter et al. (2019) and Bernasco & Block (2011) provided the raw coefficients and SE values, but Groff & Lockwood (2014) and Vilalta & Fondevila (2019) provided an IRR as well as

the SE of the IRR. Where they were not reported, standard errors (SE) were estimated using the method described in Section 3.1.6. An overall effect size was computed for each type of crime associated with the independent variables (Appendix 3-1).

3.3.1.2 Results

The results of meta-analysis are plotted on the forest plot in Figure 3-2. For each crime type, the findings from the individual studies are shown along with the overall weighted mean effect size. Findings are colour coded by crime type and independent variable considered.

The combined effect size of main roads (IRR = 1.5) on property crimes across two studies was found to be positive and significant. Two combined effect sizes for betweenness as a predictor variable were computed due to the way Kim & Wo (2023) reported their results. The least value (IRR=1.49) was insignificant while the highest value (IRR = 1.74) was significant.

For violent crimes, the IRR provided by Vilalta & Fondevila (2019) has twice the value of IRR compared to the other two studies. It is not possible to determine why this was, but it could be due to the characteristics of the study area of Mexico City, Mexico which might differ from the other two study areas which were in USA. The Santa Fe neighbourhood of Mexico City had a mixture of affluent commercial as well as residential buildings and pockets of poor areas which possibly resulted in more targets and rapid escape routes on the main road. For violent crimes, with main road as a predictor variable, the effect size (IRR=2.01) was significant and slightly higher than for property crimes. Two combined effect sizes for effect of betweenness on violent crimes were computed - lowest (IRR= 1.2, significant) and highest (IRR=1.22, significant).

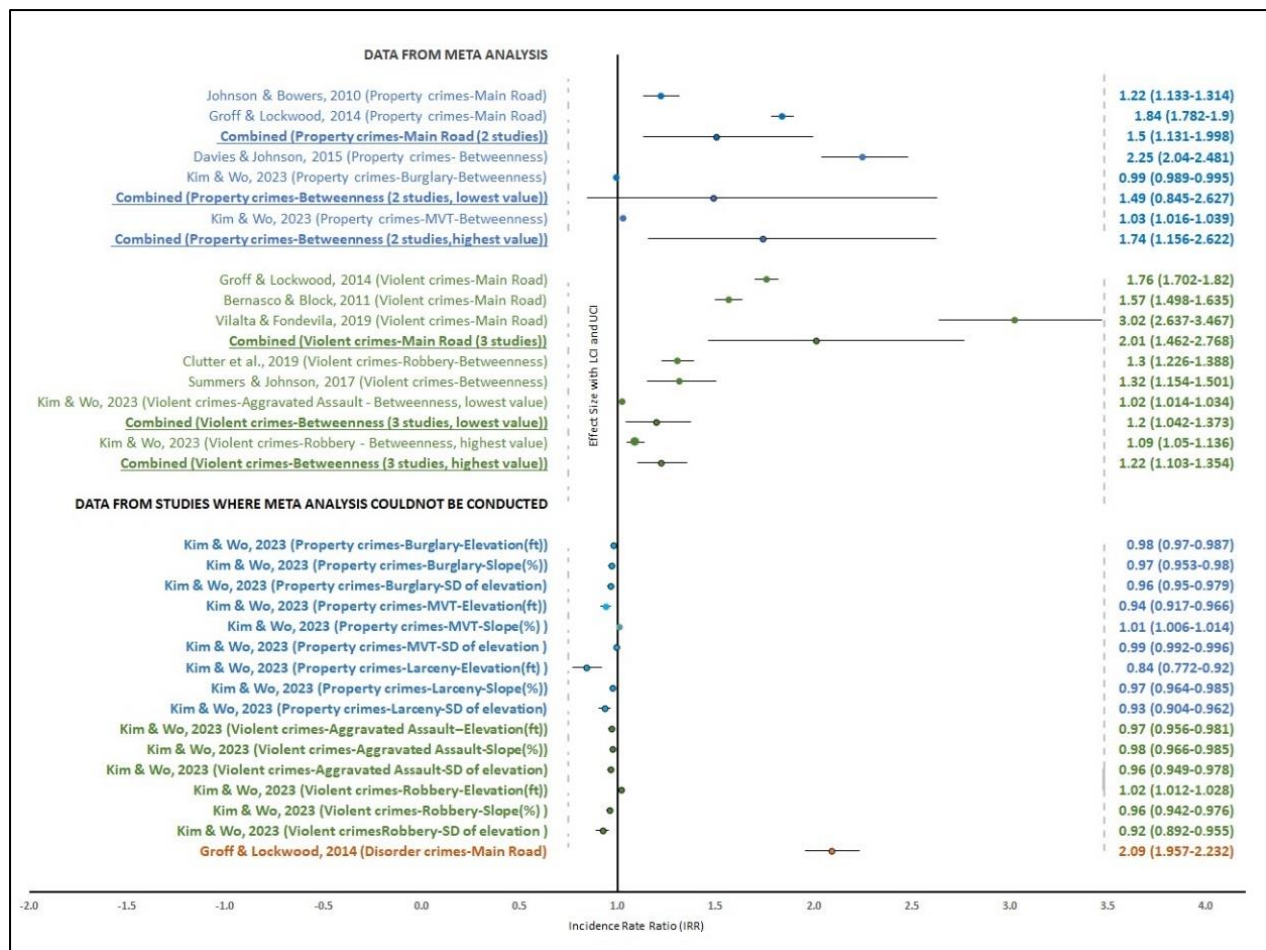


Figure 3-2 Forest plot – Influence of Street Configuration on crime

All combined effect sizes for the influence of street network, configuration and other features on crime in the forest plot correlated positively. As seen in the forest plot, five out of six confidence intervals for the estimated mean effect sizes for main roads – property & violent crimes and betweenness- violent crimes, do not overlap the null line which suggests that the influence of street configuration is not just in the positive direction but is also statistically significant, regardless of the predictor variables and crime types analysed. Notably, the effect sizes for 18 data points could not be included in the meta-analysis but were depicted on the forest plot individually. The predictor variables related to the topology of the street reduce the criminogenic effects sizes for property and violent crimes as steepness and hilliness reduce criminal opportunities as potential offenders might not be interested in the spending time and effort in hilly areas; also their routine activities usually occur elsewhere (Kim & Wo, 2023). One data point from Groff and Lockwood (2014) provided high estimate of effect of main roads on disorder crimes.

Overall, when combined meta-analytically, the findings from the studies suggest a positive association between crime and street network configurations that encourage the movement of people. This was true regardless of crime type, study location, time periods studied, the precise statistical models used, and the independent (predictor) variables included in the model specification.

3.3.2 Public Transit

Ten studies (see Table 3.5) analysed the influence of bus stops, underground / subway transit stops, tram stops and rail stations on crimes including violence, property, and drug-related offences. Four studies assessed bus stops, one study assessed bus and tram stops, three studies analysed subway stations, one study analysed train stations, and one study analysed public transit stations (without specifying the mode of transport) and found that the impact of transit areas varied by crime type. One study found bus and tram stops correlated negatively (not significant) with property and violent crimes, the remaining studies found a positive association. The studies suggested that the presence of public transit is criminogenic, and the overall effects on types of crime change depending on the location and characteristics of its environments.

Bus stops and tram stops

Six studies that examined bus transit stops found mixed results for the association with property and violent crimes, whereas overall crimes and drug crimes were positively associated with bus stops. Hsu&Miller (2017) studied the relationship between bus stops and drug dealing in Newark NJ, USA using a case-control study design. Their findings indicated that although bus stops were positively associated with crime, contrary to expectation, in terms of the crime generating capability of bus stops, the correlation between drug dealing and bus stops was not higher on intersections compared to street segments (Hsu & Miller, 2017). This study used Conditional Logistic Regression Model which was not comparable with other studies and hence was excluded from meta-analysis. Clutter et al.(2019) analysed the influence of bus stops on spatial crime patterns within BIDs of Cincinnati, USA. The authors found that street robbery was positively associated with the presence of bus stops on street segments (Clutter et al., 2019). A study in Israel found that more bus stops on the street increases property and violence crimes (Amram et al., 2024). Soohyun & Yongjei (2016) used 6975 five-ft² grid cells as the spatial unit of analysis

in Pittsburgh, USA and found a positive correlation between bus stops and all crimes (Soohyun & Yongjei, 2016). However, the multivariate linear regression model used in this study was not comparable with other studies (most studies used a count model, such as a negative binomial regression) and hence this study was not included in meta-analysis.

Favarin (2018) measured the effect of the presence of bus and tram stops in Milan, Italy on burglary and reported a negative effect size (insignificant) for the influence of transit stops on burglary. There are various reasons why the findings of this study may differ to the others. Burglaries were, however, higher when bus/tram stops were located in residential areas (Favarin, 2018). Liggett et al. (2003) looked at crime around bus stops in Los Angeles, USA. The analysis used bus stop crime and ridership data within a 150ft radius of intersections where bus stops were located to assess crimes such as rape, robbery, assault, pick pocketing, jewellery snatching, drug dealing, disorderly conduct, and public drinking. Their regression model assessed only presence of liquor store, litter, visibility and wait times. A significant positive correlation was found between overall crimes if there was a liquor stores and litter around the bus stops and the association was negative when there was sufficient pedestrian visibility in the bus stop environment (Liggett et al., 2003). Liggett et al. (2003) focussed on the crime rate for the bus stop microenvironment and considered four key variables– liquor stores near the bus stop, litter, good visibility of bus stops and wait time for bus. This was not comparable with other studies and hence was excluded from meta-analysis.

Subway and Rail stations

The findings from four studies indicate that subway, underground stops and rail stations were associated with higher crime. Groff & Lockwood (2014) studied the influence of the presence of subway stations on crimes using data for 40,371 street segments in Philadelphia, USA. The presence of subway stations was positively associated with violent, property, and disorder crime at various distance thresholds from each street segment to surrounding facilities within 400 ft, 800 ft and 1200 ft of street segments (Groff & Lockwood, 2014). As discussed in Section 3.3.1, results reported using a distances of 400 feet was included in meta-analysis as it is a smaller

Table 3.5 Influence of Public Transit on crime -- Assessment of studies for inclusion in meta-analysis

Authors and Year of Study	Crimes studied in Urban Area	Study Design	Predictor variable and correlation with crimes	Spatial unit of analysis	Effect size and precision	Statistical model	Include in meta-analysis
Amram et. Al. (2024)	Property and violence crimes in Tel Aviv-Yafo, Israel	Cross sectional study	Presence of bus stops correlated positively with property (significantly) and violent crimes	Street segment?	Provided	Zero-inflated negative binomial (ZINB) regression	Y
Groff & Lockwood (2014)	Property, Violent crimes and disorder crimes in Philadelphia, USA	Cross sectional study	Subway stops correlated positively	street segment - distance of Facilities 400 feet from street segment	Provided	Negative Binomial regression model	Y
Favarin (2018)	Property and violent crimes in Milan, Italy	Cross sectional study	Bus and Tram stops correlated negatively (not significant)	Street segment	Provided	Negative binomial regression model	Y
Bernasco & Block (2011)	Violent crimes in Chicago, USA	Cross sectional study	El stations correlated positively	Street segment	Provided	Negative Binomial Regression Models	Y
Clutter et al.(2019)	Violent crimes in Business Improvement District (BID) of Cincinnati, USA	Cross sectional study	Presence of bus stops correlated positively	Street block (segment)	Provided	Binomial Regression	Y
Haberman & Ratcliffe (2015)	Violent crimes in Philadelphia, USA	Cross sectional study	Subway stops – morning, daytime, evening, late night - correlated Positively (insignificant only in mornings)	census block	Provided	Binomial Regression Model	Y
Hsu & Miller (2017)	Drug Market crimes in Newark, USA	Matched case– control design	Bus stops correlated positively	Street segments and interactions	Provided	Conditional Logistic Regression Models	N – Statistical model is not comparable with other studies
Newton et al. (2014)	Theft of personal property / stealth crimes (property) in London underground stations, UK	Cross sectional study	internal & external features of the station and congestion of passengers correlated positively (significant)	400m buffer zone around stations	Provided	Negative Binomial Poisson regression model	N – what is measured using predictor variables such as congestion of passengers is not comparable with other studies
Liggett et al. (2003)	Violence, disorder, theft (property) and drug dealing crimes in Los Angeles, USA	Cross sectional study	presence or absence of certain characteristics of bus stops, (visibility, and lighting) and microenvironments where bus stops are located (e.g. land use around the bus stop, condition of surrounding area, street and sidewalk width, on-street parking, and traffic levels), correlated positively with crime.	46m (150ft) radius of intersections where bus stops were located	Provided	Regression analysis	N – what is measured using predictor variables such as land use around the bus stop is not comparable with other studies
Soohyun & Yongjei (2016)	All crimes - in Pittsburgh, USA	Cross sectional study	Bus stops correlated Positively (significant for property and disorder crimes, insignificant for violent crimes)	500-ft ² grid cells	Provided	Multivariate linear regression analysis	N – Statistical model is not comparable with other studies
Total studies assessed – 10, Studies included in meta-analysis – 6, Studies excluded from meta-analysis - 4							

unit. Groff & Lockwood (2014) found that the effect of subway stops on crime was reduced as the distance from the stop increased. Haberman & Ratcliffe (2015) conducted a temporal analysis using the census block as a spatial unit and demonstrated that subway stops in Philadelphia-USA subway stations were positively

associated with higher street robberies during the daytime, evening and late at night but had no influence in the morning. Robberies were also higher when the census blocks had more residents (Haberman & Ratcliffe, 2015). Newton et al. (2014) conducted an analysis of the association between street configuration within a 400-meter buffer zone of underground transit stops in London, UK. They found that the risk of theft reduced with more domestic buildings nearby, and stations classified as terminus stations. However, the risk of theft increased with increased levels of accessibility and access to stations i.e., where there was a high percentage of roads and paths in the nearby environment (Newton et al., 2014). Newton et al. (2014) analysed theft only at underground stations based on internal & external features of the station and congestion of passengers, which was not comparable with other studies and hence was excluded from meta-analysis.

Bernasco & Block (2011) measured the influence of the Elevated (or EL) rail stations (meaning a station for rapid-transit system) in Chicago, USA on street robberies. They found that census blocks with an EL rapid transit system station had more than 4 times as many robberies as similar blocks without a public rail station (Wim Bernasco & Block, 2011).

3.3.2.1 Data synthesis

Seven studies were divided into 3 groups according to the types of crime they examined. The predictor variables used in all studies were transit stops and hence no further grouping was required based on the predictor variables. The grouping of data from studies based on crime types is summarised below (see Table 3.6).

The statistics that could be extracted from the studies were analysed to calculate overall combined effect sizes where meta-analysis could be conducted (Appendix 3-2). Favarin (2018) reported an IRR and a Coefficient but did not provide a SE or t or z statistics. Consequently, the only way to compute a SE was to use the p-value. However, the results were non-significant and consequently a specific p value was not provided. For this reason, two estimates of the overall effect size were computed using the potential highest ($p=0.51$, $IRR = 1.93$) and lowest values of p ($p=0.1$, $IRR = 0.98$) (see Fig 3.3), and both were included in the forest plot. Haberman & Ratcliffe (2015) measured the influence of subway stops of Philadelphia (USA) on

Table 3.6 Data Analysis-Influence of Public Transit on crime grouped by predictor variable and crime type

Authors and Year of Study	Included in Meta-analysis	Included in Forest plot
Property crimes (3 studies)		
Groff & Lockwood (2014)	Y	Y
Favarin (2018)	Y	Y
Amram et. Al. (2024)	Y	Y
Violent crimes (6 studies)		
Groff & Lockwood (2014)	Y	Y
Favarin (2018)	Y	Y
Bernasco & Block (2011)	Y	Y
Clutter et al. (2019)	Y	Y
Haberman & Ratcliffe (2015)	Y	Y
Amram et. Al. (2024)	Y	Y
Disorder crimes (1 study)		
Groff & Lockwood (2014)	N	Y

robbery across four time periods – morning, daytime, evening, and late night. The effect sizes varied marginally across all four time periods. The effect sizes were insignificant in the morning and in the evening however, the effects were somewhat significant during daytime and highly significant during late night USA (Haberman & Ratcliffe, 2015b). Rather than use only one data point from this study, the overall effect size was computed for both the highest and lowest effect size values (providing best- and worst-case scenarios). Hence for violent crimes, effect sizes from six studies with comparable findings were combined in the meta-analysis.

3.3.2.2 Results

The results of the meta-analysis are shown in Figure 3-3. For each crime type, the findings from the individual studies are shown along with the overall weighted mean effect size. Findings are again colour coded by crime type and independent variable considered.

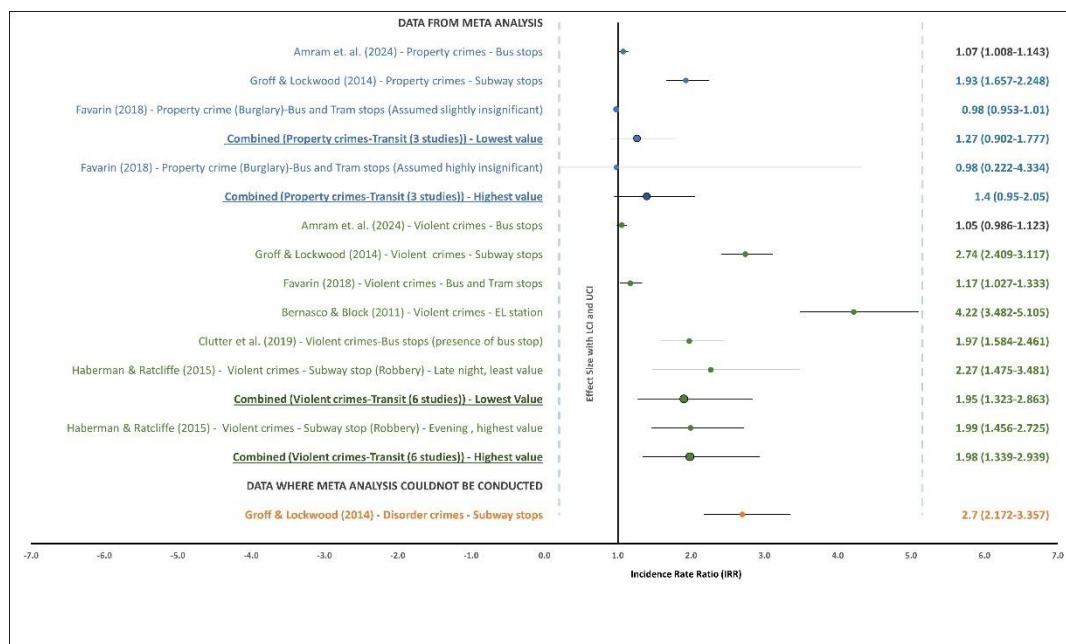


Figure 3-3 Forest plot – Influence of Public Transit on crime

As seen in the forest plot, the combined effect sizes for the effect of public transit on property and violent crimes are positive. Two estimates of the overall effect size were computed for property crimes due to the way that Favarin (2018) reported results (see above). For property crimes, the combined effect sizes (combined values of IRR = 1.27 being the lowest and IRR=1.4 being the highest) were found to be positive and insignificant. Two estimates of the overall effect size for violent crimes were computed due to the way Haberman & Ratcliffe (2015) reported results (see above). For the violent crimes, the two mean effect sizes (measured in morning and evening) that were computed in both cases were similar (least combined value of IRR = 1.90 and highest combined value of IRR =1.98) and were highly significant. Groff & Lockwood (2014) was the only study that analysed the influence of subway stops on disorder crimes (IRR=2.7), wherein the effect size was in the positive direction. Overall, the findings of the meta-analysis suggest that the effect of public transit stops on property crimes are lower than they are for violent and disorder crimes regardless of public transit types (bus, tram, rail, and subway stops), time of travel and distance from public transit facilities.

3.3.3 Parks

Five studies assessed the influence of parks on violent, property, drug and disorder crimes within parks and the surrounding areas (see Table 3.7). Two studies indicated that the park environments are positively associated with crime, one study showed a

negative association, one study showed no correlation, and one study showed mixed results.

Groff & McCord (2012) studied violent, property and disorder crimes in Philadelphia, USA parks and found that crime counts in the parks and their surrounding streets were double than the other areas with disorder crimes being higher than violent and property crimes. Analysis of 400-1200 feet buffer areas surrounding the parks suggested that parks were associated with decreased crime in the immediate vicinity (0-400 feet) and far away (800-1200 feet) but that there was an increase in crime in the area 400-800 feet buffer area in between (Groff & Mccord, 2012). The built environment characteristics and activity generators within the park environment showed different associations for different types of crime. Parks with tennis courts and basketball courts were associated with reduced property and violent crime; basketball courts were associated with increased disorder and other courts were associated with increased violence. The presence of recreation centres and public transit stops were associated with reduced disorder crime but did not show any effect on violent or property crime. However, overall, activity generators were associated with lower levels of crime. Increased residential land use surrounding the parks was correlated with higher levels of crime (Elizabeth R Groff & Mccord, 2012). This study examined crime correlated with activity generators in the parks, which was not comparable to other studies. Hence this study was excluded from the meta-analysis.

One study reported the findings from a spatio temporal analysis and found that parks were correlated with higher property and violent crimes in spring and summer seasons. In their study of street robbery patterns in Philadelphia, USA, Haberman & Ratcliffe (2015) found a significant positive correlation with neighbourhood parks and crime at the census block level at all times of the day. The neighbourhood parks were associated with crimes across four time periods – morning, daytime, evening and late night (except the late-night hours) during the spring and summer seasons (Haberman & Ratcliffe, 2015). The effect sizes did not vary largely across the time periods; however, the effect size was higher in the daytime, but lower during mornings, evenings, and night-time (Haberman & Ratcliffe, 2015). The nearby blocks experienced spillover effects during the late-night hours (Haberman & Ratcliffe, 2015). Aggravated assault and homicide were significantly and positively associated with the presence of a park in a block. Robbery, larceny, motor theft and homicide had a

significant negative correlation with blocks that were within 400 feet of a park. Notably, the size of a park had no significant association with any predictor variables.

Table 3.7 Influence of Parks on crime – Analysis of studies for inclusion in meta-analysis

Authors and Year of Study	Crimes studied in Urban Area	Study Design	Predictor variable and correlation	Spatial unit of analysis	Effect size and precision	Statistical Model	Included in meta-analysis
Boessen et. al (2018)	Property crimes (Burglary, Motor Theft, Larceny, Violent crimes (Robbery, Aggravated Assault and Homicide) in Chicago, Cleveland, Columbus, Dallas, Los Angeles, Milwaukee, Oakland, San Francisco, and Tucson (USA)	Longitudinal study	a) Block with a park had significant positive association with Aggravated Assault; rest was insignificant b) When block is within 400 feet of park there was significant negative correlation with Larceny, Motor theft and Homicide; rest was insignificant c) Size of park – no significant correlation	Census block	Provided	Negative Binomial Regression Model	Y Data points that measured association of predictor variables (such as Block with a park) with crimes are not comparable to other studies and hence were excluded, other data was included in meta-analysis
Clutter et al.(2019)	Robbery (Violent) crimes in Business Improvement District (BID) of Cincinnati, USA	Cross sectional study	Presence of parks had negative effect size (insignificant)	Street block (segment)	Provided	Binomial Regression	Y
Haberman & Ratcliffe (2015)	Robbery (Violent) crimes in Philadelphia, USA	Cross sectional study	Presence of parks – morning, daytime, evening, late night - correlated positively (insignificant only in late night)	Census block	Provided	Binomial Regression Model	Y
Hsu&Miller (2017)	Drug Market crimes in Newark, USA	Matched case-control design	Public parks showed no correlation	Street segments and interactions	Provided	Conditional Logistic Regression Models	N- statistical model is not comparable with other studies
Groff & Mccord (2012)	Property, Violent and disorder crimes in Philadelphia, USA	Cross sectional study	Rate of crime in parks and surrounding area is higher compared to the remainder of the city	Park and a 50foot buffer around the park	Provided	ANOVA	N – what is being measured by predictor variables such as crime in areas surrounding the parks is not comparable to other studies
Total studies assessed – 5, Studies included in meta-analysis – 3, Studies excluded from meta-analysis -2							

Clutter et al.(2019) studied patterns of robbery in the BID of Cincinnati, USA using street segments as the spatial unit of analysis. This cross sectional study found a negative correlation between parks on street segments and the volume of robbery (Clutter et al., 2019). The high street usage in the study area - Business Improvement Districts (BIDs) of Cincinnati, USA could have contributed to lower robberies.

Hsu & Miller (2017) analysed the differences in situational factors between street segments and intersections that are associated with drug-dealing in Newark, USA. They found that public parks were not associated with drug markets across street segments and intersections (Hsu & Miller, 2017). This study used a Conditional Logistic regression model which is not comparable with other studies that used Negative Binomial Regression. Hence this study was excluded from meta-analysis.

Boessen et. al (2018) analysed crime data for aggravated assault, robbery, homicide, burglary, motor vehicle theft, and larceny crimes using the census block as

the spatial unit for nine cities in the USA (Chicago, Cleveland, Columbus, Dallas, Los Angeles, Milwaukee, Oakland, San Francisco, and Tucson). The predictor variables included the presence of a park in a block, the size of a park and proximity to parks. The crime types examined included violent crimes (Robbery, Aggravated Assault and Homicide), property crime (Burglary, Motor theft and Larceny) and drug market crimes. They found that residential areas in blocks with parks were associated with higher levels of crimes, but the effect did not depend upon the size of the park; however, the level of crimes reduced as distance from the park increased (Boessen et al., 2018). Blocks with commercial, industrial and office areas were associated with higher crime; however the crime rates were lower compared to residential blocks (except for violence) and, the crime rate did not change due to proximity to a park (Boessen et al., 2018).

3.3.3.1 Data synthesis

Data from the four included studies were grouped according to the predictor variables used and the types of crime studied (see Table 3.8).

Table 3.8 Data Analysis-Influence of Parks on crime grouped by predictor

Authors and Year of Study	Included in Meta-analysis	Included in Forest plot
Multiple data points for Property crimes (Burglary, Motor theft and Larceny) with predictor variables that are not comparable (Block has a park, size of park, Block is within 400 ft of park)		
Boessen et. al (2018)	N	Y
Predictor variable Block has a park – Robbery (Violent crimes) - (3 studies)		
Boessen et. al (2018)	Y	Y
Clutter et al.(2019)	Y	Y
Haberman & Ratcliffe (2015)	Y	Y
Multiple data points for Violent (Robbery) crimes with predictor variables that are not comparable (size of park,), Property crimes (Aggravated Assault and Homicide) with predictor variables that are not comparable (Block has a park, size of park, Block is within 400 ft of park)		
Boessen et. al (2018)	N	Y

The data for property (separately for burglary, motor theft and larceny) and violent crimes (separately robbery, aggravated assault, and homicide) from Boessen et. al (2018) were extracted to understand the effect of the presence of a park in the block, crime at 400m distance from a park and whether there was any variation in the association with crime based on the size of the park. Haberman & Ratcliffe (2015) conducted a spatio-temporal analysis, hence the lowest and highest effect sizes from this study were used to compute a combined effect size (for the best-case and the

worst-case scenarios). The remaining data that could not be included for meta-analysis consisted of only one effect size for each crime type-predictor variable combination.

The statistics that could be extracted from the studies were analysed to calculate overall combined effect sizes where possible (see Appendix 3-3).

3.3.3.2 Results

Figure 3-4 shows a forest plot for the influence of parks on crime. The individual effect sizes and their confidence intervals are plotted along with the overall mean effect size, where appropriate.

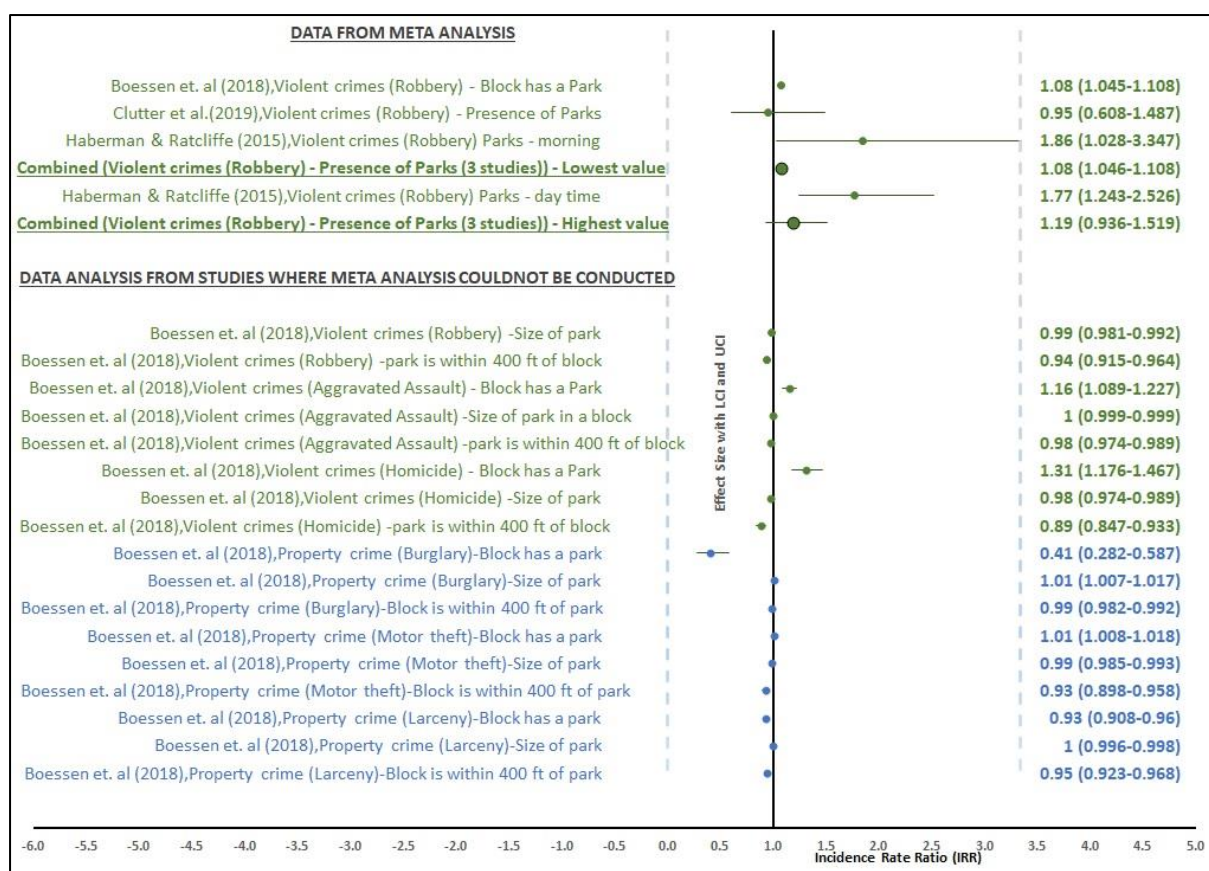


Figure 3-4 Forest plot for Influence of Parks on crimes

Multiple data points for the effect of parks on specific crime types were plotted on the forest plot (Figure 3-4). The effect sizes for robbery crimes were varied (IRR = 0.95 to 1.77) and could only be meaningfully combined across three studies. The combined effect of parks on robbery was positive (combined values of IRR = 1.08 being the lowest but significant, and 1.19 being the highest and insignificant). The lowest significant effect size was associated with morning times when there are less

people in and around parks who can act as guardians or place managers. The highest effect size was associated with daytime in parks where there are usually many people can act as guardians or place managers, which could be the reason for the effect size to be insignificant. The effect sizes of the remaining predictor variables for property and violent crimes were plotted for only one study - Bossen et al. (2018). and had small values (IRR varied from .41 to 1.31).

The results of this meta-analysis need to be treated with caution due to a small number of data points included in this study. More data is required to conduct a conclusive meta-analysis for the influence of parks on crime.

3.3.4 Schools

Seven studies analysed the association between various types of schools and crime for property, theft, and violent crime (see Table 3.9). All studies showed a positive correlation of schools with multiple crime types, however, levels of statistical significance varied.

Soohyun & Yongjei (2016) used 6975 five-ft² grid cells overlaid on the city of Pittsburgh, USA and found a positive correlation between the count of schools with violence, property and all crimes. Clutter et al. (2019) studied the influence of schools within the BID of Cincinnati, USA. They assessed high schools and location of higher education schools and found that both correlated positively with levels of robbery (Clutter et al., 2019). Groff & Lockwood (2014) studied the exposure of street segments to non-elementary schools (at a threshold distance of 400 feet) on property crimes. The authors found that the non elementary schools were significantly associated with disorder offenses however, the effect on violent and property crimes was positive, but insignificant (Groff & Lockwood, 2014). Favarin (2018) measured how the total number of schools within a buffer of 100 metres correlated with (property) crimes in Milan, Italy. The study found that schools that are on a street segment or intersect with street segments showed positive correlation with street robbery (Favarin, 2018). Wo and Park (2020) conducted a census block-level analysis of schools and its correlation with crime in Chicago, USA. They found that the presence of any school in a block was correlated positively and significantly with property and violent crimes (Wo & Park, 2020). To be consistent across studies, the results from Model 5 were included for meta-analysis as this model incorporated a range of socio-demographic and socio-economic characteristics in the block (as in other studies).

Table 3.9 Influence of Schools on crime –Analysis of studies for inclusion in meta-analysis

Authors and Year of Study	Crimes studied in Urban Area	Study Design	Predictor variable and correlation with crimes	Spatial unit of analysis	Effect size and precision	Statistical model	Include in meta-analysis
Soohyun & Yongjei (2016)	All crimes - in Pittsburgh, USA,	Cross sectional study	All schools (kindergartens, elementary, high schools) correlated positively (significant for property and all crimes)	500-ft ² grid cells	Provided	Multivariate linear regression analysis	N- statistical model is not comparable with other studies
Favarin (2018)	Property crimes in Milan, Italy	Cross sectional study	Schools correlated positively (Not significant)	Street segment	Provided	Negative binomial regression model	Y
Haberman & Ratcliffe (2015)	Violent crimes in Philadelphia, USA	Cross sectional study	High schools – morning, daytime, evening, late night - correlated positively (significant except in the morning)	census block	Provided	Binomial Regression Model	Y
Groff & Lockwood (2014)	Property, Violence and disorder crimes in Philadelphia, USA,	Cross sectional study	Non elementary schools correlated positively for property and violence (insignificant) and disorder crimes (significant)	Street segment	Provided	Negative binomial regression model	Y
Clutter et al. (2019)	Robberies (Violent) crimes in Business Improvement District (BID) of Cincinnati, USA	Cross sectional study	High school had positive effect size (insignificant) and higher education correlated (significantly)	Street block (segment)	Provided	Binomial Regression	Y
Kim & Wo (2022)	Seasonal influence of robbery, aggravated assault (Violent) crimes; burglary larceny, and motor vehicle theft (property) crimes in Orlando, USA	Cross sectional study	Correlated positively, risk of crime (especially aggravated assault) peaks during the summer-fall weeks.	Census block	Provided	Logistic Regression	N- statistical model is not comparable with other studies
Wo & Park (2020)	Property and violent crimes in Chicago, USA	Cross sectional study	Schools correlate positively and significantly	Census block	Provided	Negative Binomial Regression	Y
Total studies assessed – 7, Studies which could be included in meta-analysis – 5, Studies excluded from meta-analysis - 2							

Two studies-Haberman & Ratcliffe (2015) and Kim & Wo (2022) found that the correlation between schools and crime was positive. In their analysis (see above), Haberman & Ratcliffe (2015) found that crime was higher in census blocks of Philadelphia, USA containing schools not just during the time they were open but also during the times that they were “unofficially” not in use (Haberman & Ratcliffe, 2015). It was observed that the effect sizes were very similar across all day and night times. Kim & Wo (2022) found that schools in Orlando, USA have a non-linear higher

association with property and violent crimes. Crime peaks during summer and fall seasons where schools are not in session (Kim & Wo, 2022).

Soohyun & Yongjei (2016) and Kim & Wo (2022) used statistical models (Multivariate linear regression analysis and Logistic Regression respectively) that were not comparable to other studies and hence were excluded from meta-analysis.

3.3.4.1 Data Synthesis

Studies were divided into groups according to the types of crime they examined (see Table 3.10).

Table 3.10 Data Analysis-Influence of schools on crime grouped by predictor variable and crime type

Authors and Year of Study	Included in Meta-analysis	Included in Forest plot
Property crimes, Predictor variable - schools (2 studies)		
Groff & Lockwood (2014)	Y	Y
Favarin (2018)	Y	Y
Violent crimes, Predictor variable - schools (3 studies)		
Groff & Lockwood (2014)	Y	Y
Clutter et al. (2019)	Y	Y
Haberman & Ratcliffe (2015)	Y	Y
Violent crimes, Predictor variable – Higher education (1 study)		
Clutter et al. (2019)	N	Y
Disorder crimes, Predictor variable - schools (1 study)		
Groff & Lockwood (2014)	N	Y

The data extracted from the studies were analysed to calculate overall combined effect sizes where it was possible to do so (see Appendix 3-4). Favarin (2018) reported an IRR and a coefficient but did not provide a SE, t, z, or p value. Consequently, two effect sizes were calculated based on the assumed highest and least insignificant values. Haberman & Ratcliffe (2015) conducted a spatio-temporal analysis. The lowest effect size in the late night and the highest effect size in the evening were used to compute a combined effect size (for the best- and worst-case scenarios).

3.3.4.2 Results

Figure 3-5 shows a forest plot for the influence of the presence of schools on crime.

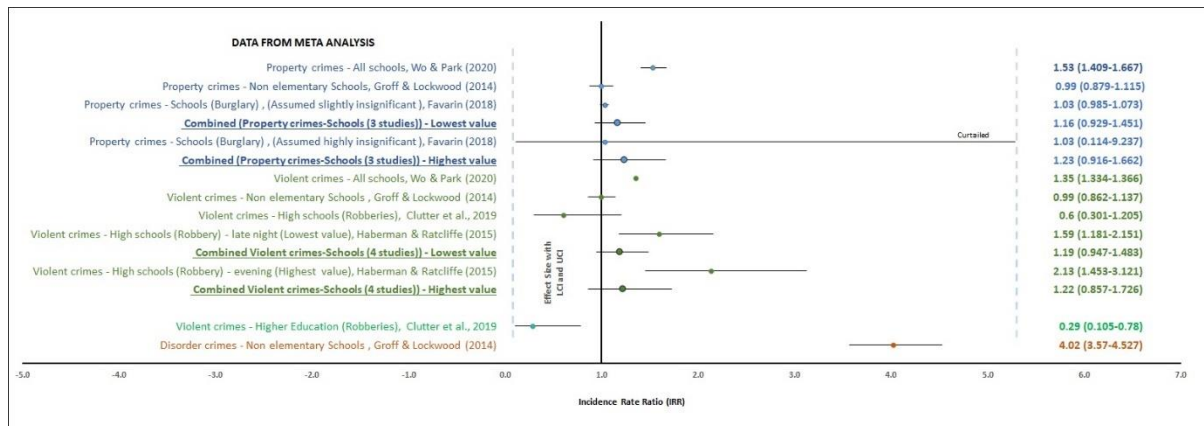


Figure 3-5 Forest plot for Influence of schools on crimes

Although only 3 data points were found for property crimes, the IRR ranged from 0.99 to 1.53 which was quite varied. Wo & Park (2020) had comparatively highest effect size of effect of schools on crimes. This could be because they considered all public and private schools in Chicago, USA. For property crimes, two estimates of the overall effect size were computed due to the way that Favarin (2018) reported the results. As seen in the forest plot, both the lowest combined effect size for property crimes (IRR=1.16) and highest (IRR=1.23), were positive but not large values, and were not statistically significant.

For violent crimes, data from four studies was suitable for meta-analysis. The lowest and highest combined effect sizes (IRR= 1.19 and 1.22 respectively) were both statistically insignificant. Groff & Lockwood (2014) assessed disorder crimes and found a significant criminogenic effect of schools (IRR=4.02). However, this result is inconclusive as it is from only one study.

In conclusion, the results of the meta-analysis indicated that the overall estimated effect of schools on property and violent crimes were positive, similar, low and not statistically significant. The reason could be attributed to the types of schools assessed (public, private, kindergarten to universities), seasonal impacts and youths not attending the school but committing crimes in nearby facilities. Overall, the findings reported here need to be validated with more data points from further research.

3.3.5 Alcohol outlets

Ten studies analysed the relationship between crime and drinking establishments, such as alcohol outlets, eating & drinking establishments, liquor stores and bars (see Table 3.11). All studies revealed a positive correlation with violent crimes and the effect was found to extend beyond the alcohol outlets.

Clutter et al. (2019) studied whether the location of alcohol establishments in the BID studied were associated with spatial crime patterns in Cincinnati, USA. They found that the count of alcohol establishments within a BID had a positive association with violent crime, however, the association was insignificant (Clutter et al., 2019).

Vilalta & Fondevila (2019) studied crime risks in structurally advantaged as well as disadvantaged census blocks to examine the influence of drinking places on the distribution of violent crime. This study, conducted in Santa Fe neighbourhood, Mexico City, Mexico found that violent crime was positively associated with the count of on-premises and off-premise alcohol outlets, but crime was higher in the blocks with business outlets (Vilalta & Fondevila, 2019).

In their study that used census blocks as a spatial unit of analysis, Bernasco & Block (2011) found that the count of Liquor stores as well as bars in Chicago, USA, correlated positively with robberies. The findings indicated that the effect extended to the adjacent blocks as well as those that were farther away. The association at all distances was higher if crime attractors (such as places for illegal drug markets or prostitution) and crime generators (such as bus stops, parking places and supermarkets) were present in the block and decreased where relatively fewer numbers of crime attractors and crime generators were present on the blocks. They found that the addition of one liquor store was associated with a 67% rise in the robbery crime risk of the block (Wim Bernasco & Block, 2011).

Table 3.11 Influence of Alcohol outlets on crime – Analysis of studies for inclusion in meta-analysis

Authors and Year of Study	Crimes studied in Urban Area	Study Design	Predictor variable and correlation with crimes	Spatial unit of analysis	Effect size and precision	Statistical model	Include in meta-analysis
Groff & Lockwood (2014)	Property, Violence and disorder crimes in Philadelphia, USA	Cross sectional study	Bars correlated positively	Street segment	Provided	Negative binomial regression model	Y
Favarin (2018)	Property and violent crimes in Milan, Italy	Cross sectional study	Licensed premises correlated positively	Street segment	Provided	Negative binomial regression model	Y
Groff (2014)	Violent crimes in Seattle, USA	Cross sectional	Alcohol outlets measured using weightage based on the distance from a street segment correlated positively	Street segment (distance of 400 feet)	Provided	ZINB regression Negative Binomial	N- what is being measured by predictor variables (using weightage) is not comparable to other studies
Bernasco & Block (2011)	Violent crimes in Chicago, USA	Cross sectional study	Number of bars and clubs with less than 10 employees and no of liquor stores correlated positively	Street segment	Provided	Negative Binomial Regression Models	Y
Clutter et al.(2019)	Violent crimes in Business Improvement District (BID) of Cincinnati, USA	Cross sectional study	Drinking places had positive effect size (insignificant)	Street block (segment)	Provided	Binomial Regression	Y
Vilalta & Fondevila, (2019)	Violent crimes in Santa Fe, Mexico city, Mexico	Cross sectional study	Alcohol outlets correlated Positively	census block	Provided	Mixed Poisson Geographically Weighted Regression (GWPR)	Y
De Souza & Miller (2012)	Violent crimes in Belo Horizonte, Brazil	Matched case control study	Bars - overall effect, daytime, night-time - correlated positively	50 m to 100-meter area from homicide address	Provided	Ordinary least squares fixed effect Linear Regression model	N- statistical model is not comparable with other studies
Haberman & Ratcliffe (2015)	Violent crimes in Philadelphia, USA	Cross sectional study	Alcohol stores and bars – morning, daytime, evening, late night - had positive effect size (insignificant)	census block	Provided	Binomial Regression Model	Y
Liggett et al. (2003)	Violence, disorder, theft (property) and drug dealing crimes in Los Angeles, USA	Cross sectional study	Presence of liquor stores correlated positively with bus stops at intersections	46m (150ft) radius of intersections where bus stops were located	Provided	Regression analysis	N – compared crime rates between two urban elements, not comparable with other studies
Ratcliffe (2012)	Violent crimes in Philadelphia, USA	Cross sectional study	Bars, on-site consumption open to the public only, 8 PM–4 AM correlated positively	85 feet from centroid of the bars	(Detects change in regression coefficient for distance thresholds. Absolute effect size is not provided)	Change point Poisson regression	N – Effect size not provided
Total studies assessed – 10, Studies included in meta-analysis – 6, Studies excluded from meta-analysis - 4							

Liggett et al. (2003) studied violent crimes in Los Angeles, USA in a 150ft radius of intersections where bus stops were located. They found that the presence of liquor stores correlated positively with alcohol outlets at bus stops at intersections. What was measured in this study was not comparable with other studies and hence this study was not included in the meta-analysis. Ratcliffe (2012) analysed the influence of bars at distance thresholds of 85, 420, and 540 feet and concluded that alcohol outlets were significantly correlated with violent crime within 85 feet of the outlets, and this association was insignificant at distances greater than 85 feet (Ratcliffe, 2012).

However, this study was not included in meta-analysis as effect sizes were not provided.

Groff (2014) studied two measures to model the influence of alcohol facilities on violent crime on street segments. The first was the count of drinking places within seven distance thresholds of a street segment (400, 800, 1200, 1600, 2000, 2400, 2800 feet). For the second measure, termed as inverse distance weighted count, each alcohol outlet within a threshold was assigned weightage based on the distance from a street segment. This study conducted in Seattle, USA found that both measures (of drinking outlet density) were positively associated with violent crime, but that the effect reduced with distance. The inverse distance weighted count was the best fitting model wherein the effect of drinking places persisted up to 2800 feet. These findings suggest that the influence of drinking establishments on crime extends to surrounding streets (Groff, 2014). However, the methods for measuring the effects of alcohol establishments on crime are not comparable to other studies. Hence this study was excluded from the meta-analysis.

Favarin (2018) analysed the association between burglary and robbery and the total number of licensed premises on Milan's (Italy) street segments. The licensed premises included all premises such as bars, restaurants and night clubs that had a licence to serve alcohol. It was concluded that there is a positive association of licenced premises with both burglary and robbery (Favarin, 2018). Groff & Lockwood (2014) studied the influence of bars on violent crimes, property crime, and disorder crimes. They used the street segment as the unit of analysis and found that all crimes were associated with these facilities at all distance thresholds considered (Groff & Lockwood, 2014).

Two studies conducted a spatio-temporal analysis. Haberman & Ratcliffe (2015) analysed data for Philadelphia, USA for 4 different time periods (morning, daytime, evening, and late night), to see if crime concentrates around alcohol establishments and if this is higher in the evening than during the daytime. It is noteworthy that the effect size for bars was positive and lowest in the evening, whereas the effect sizes for alcohol stores was negative and lowest in the morning; both bars and alcohol stores had the highest association with robbery during the daytime (Haberman & Ratcliffe, 2015b). Haberman & Ratcliffe argued that this was due to steady usage patterns. De Souza & Miller (2012) conducted a matched-case control study in Belo Horizonte, Brazil's poor urban towns known as favelas studied the effect

of bars on violent crimes during the day and night-time. Comparisons were made of the situational characteristics of a sample of 100 addresses where homicide had occurred and 100 control locations where it had not. Data on homicides in the favelas were gathered using field observations, documents, and interviews with police officers. To examine the influence of facilities, they examined what types of properties were found within 50 meters (min) and 100 meters (max) of the sample addresses. They found that the correlation was greater for homicides committed during the daytime and evening than at night-time (De Souza & Miller, 2012). However, De Souza & Miller (2012) used an Ordinary least square fixed effect Linear Regression model which is not comparable with other studies and hence this study was excluded from the meta-analysis.

3.3.5.1 Data synthesis

Studies were further grouped based on predictor variables and crime type. The predictor variables used in the studies included the number of licenced premises for alcohol consumption (such as bars, restaurants, clubs), number of liquor stores and distance of alcohol outlets from street segments. The aim of the meta-analysis was to compute the combined effect of the presence of all types of on-premises and off-premises alcohol outlets. Hence the data was not analysed further based on alcohol establishment type. The grouping of data from studies based on crime types is summarised below (see Table 3.12).

Table 3.12 Data Analysis-Influence of Alcohol outlets on crime grouped by predictor variable and crime type

Authors and Year of Study	Included in Meta-analysis	Included in Forest plot
Property crimes (2 studies)		
Groff & Lockwood (2014)	Y	Y
Favarin (2018)	Y	Y
Violent crimes (6 studies)		
Groff & Lockwood (2014)	Y	Y
Favarin (2018)	Y	Y
Clutter et al. (2019)	Y	Y
Bernasco & Block (2011)	Y	Y
Vilalta & Fondevila (2019)	Y	Y
Haberman & Ratcliffe (2015)	Y	Y
Disorder crimes (1 study)		
Groff & Lockwood (2014)	N	Y

The statistics were extracted from the studies and an overall effect size computed where data were comparable (see Appendix 3-5). The effect for two studies

that focussed on property crimes were positive in direction (significant) and were combined in the meta-analysis. Bernasco & Block (2011) measured two separate effect sizes for the influence of the number of licenced premises (bars and clubs) as well as the number of Liquor stores in Chicago (USA) on violent crimes (Wim Bernasco & Block, 2011). The lowest and highest effect sizes from this study were included in meta-analysis. Similarly, the lowest mean effect size (in the evening) as well as the highest mean effect size (daytime) of bars and alcohol stores as reported by Haberman & Ratcliffe (2015) were also included in the meta-analysis.

3.3.5.2 Results

The individual IRRs, their confidence intervals, and the overall mean effect size, where appropriate were plotted on a forest plot (see Figure 3-6).

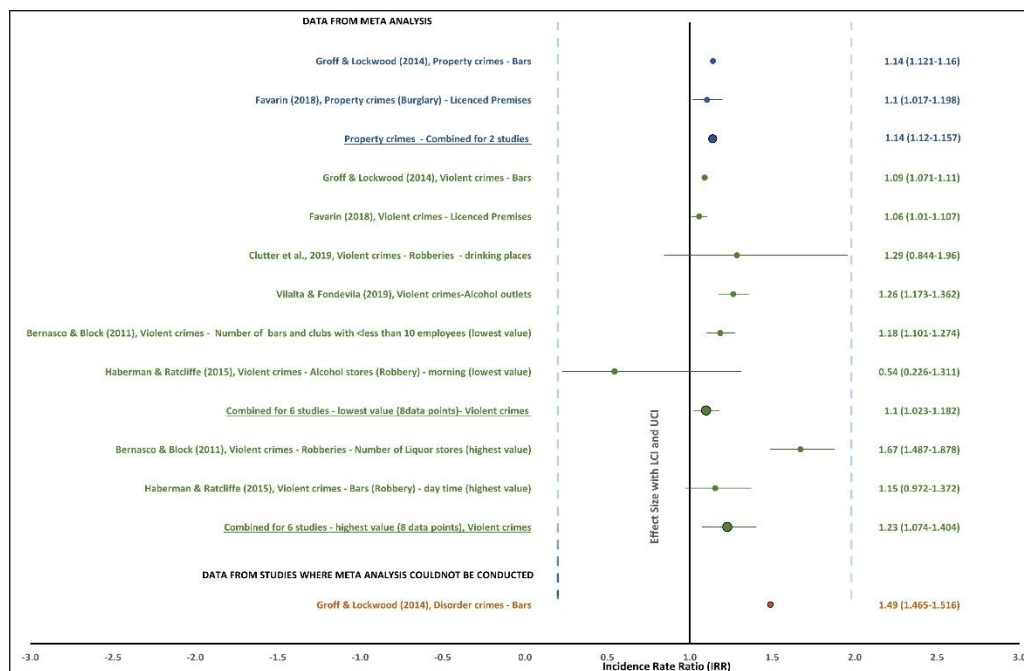


Figure 3-6 Forest plot for Influence of Alcohol outlets on crimes

As seen in the forest plot, for property crimes, the combined effect size (IRR = 1.14) showed significant positive correlation with alcohol outlets. The results need to be treated with caution as the meta-analysis was done for data from only two studies. For violent crimes, six data points were available, the effect sizes for which varied (IRR = 0.54 to 1.67). The combined effect size of alcohol outlets on violent crimes was also statistically significant and in positive direction (IRR = 1.10 being the lowest and IRR=1.23 being the highest). Groff & Lockwood (2014) was the only study that

provided data for disorder crimes. The effect size (IRR = 1.49) was positive and significant.

Overall, the results of the meta-analysis indicated that the combined effect of alcohol outlets on property, and violent crimes were similar (IRR ranged from 1.14 to 1.23). This could be because the studies mainly assessed robberies as violent crimes. The results could have been different if other types of crimes such as assault and disorder were analysed by more studies. When combined meta-analytically, the results generally suggest that the presence of alcohol outlets is associated with crimes regardless of the type of outlet, location, methods used to estimate effect sizes, and the statistical models used for calculations. However, more studies are required to estimate the effect of alcohol outlets on crimes.

3.3.6 Retail land use

Eleven studies examined the effect of retail land use such as grocery, corner store (including restaurants, or takeaway outlets on crime (see Table 3.13). All studies correlated positively with the offences studied.

Table 3.13 Influence of Retail land use on crime – Analysis of studies for inclusion in meta-analysis

Authors and Year of Study	Crimes studied in Urban Area	Study Design	Predictor variable and correlation with crimes	Spatial unit of analysis	Effect size and precision	Statistical Model	Include in meta-analysis
Soohyun & Yongjei (2016)	All crimes - in Pittsburgh, USA	Cross sectional study	Retail land use correlated positively	500-ft ² grid cells	Provided	Multivariate linear regression analysis	N- statistical model is not comparable with other studies
De Souza & Miller (2012)	Violent crimes in Belo Horizonte, Brazil	Matched case control study	Commercial Stores - overall effect, effect at night - correlated positively (not significant), daytime - correlated negatively (not significant)	50 m to 100-meter area from homicide address	Provided	Ordinary least squares fixed effect Linear Regression model	N- statistical model is not comparable with other studies
Bowers (2014)	Theft from person (snatches, pick pocketing, other theft) – internal and external to facilities in a metropolitan city centre of UK	Cross sectional study	External thefts had a positive insignificant effect size	50x50 metre grid cells	Provided	Spatial Regression model	Y
Hsu&Miller (2017)	Drug Market crimes in Newark, USA	Matched case– control design	Retail facility correlated positively	Street segments and interactions	Provided	Conditional Logistic Regression Models	N- statistical model is not comparable with other studies
Bernasco & Block (2011)	Robbery (Violent crimes) in Chicago, USA	Cross sectional study	Retail businesses correlated positively	Street segment	Provided	Negative Binomial Regression Model	Y
Clutter et al, (2019)	Street robbery (Violent crimes) in Business Improvement District (BID) of Cincinnati, USA	Cross sectional study	Every additional day store correlated positively	Street blocks (segments)	Provided	Negative Binomial regression model	Y
Haberman & Ratcliffe (2015)	Violent crimes in Philadelphia, USA	Cross sectional study,	Corner stores and fast-food restaurants—morning, daytime, evening, late night—correlated positively	census block	Provided	Binomial Regression Model	Y
Vilalta & Fondevila, (2019)	Violent crimes in Santa Fe, Mexico city, Mexico	Cross sectional	Stores- effect size was positive (insignificant)	census block	Provided	Mixed Geographically Weighted Poisson Regression (GWPVR)	Y
Favarin (2018)	Property and violent crimes in Milan, Italy	Cross sectional	Retail shops and Personal care shops correlated Positively	Street segment	Provided	Negative binomial regression model	Y
Kim & Hipp, (2019)	Burglary (Property) crime - Acquisitive crimes (and violence) in Southern California region, USA	Cross sectional study	Betweenness on the local scale of 1/4 mile and 1 mile correlated positively	Street segment	Provided	Negative Binomial Regression model used non-linear (curvilinear) relationship between street activity and crime levels	N- statistical model is not comparable with other studies
Kim & Vvo (2022)	Seasonal influence of robbery, aggravated assault (Violent) crimes; burglary larceny, and motor vehicle theft (property) crimes in Orlando, USA	Cross sectional study	Blocks with Stores, and restaurants correlated positively with seasonal patterns, risk of crime peaks during the summer-fall weeks.	Census block	Provided	Logistic Regression	N- statistical model is not comparable with other studies
Total studies assessed – 11, Studies included in meta-analysis – 6, Studies excluded from meta-analysis - 5							

Bernasco & Block (2011) conducted a spatial analysis to understand if retail stores within census blocks were associated with robberies in Chicago. A subset of nine types of shops and businesses were selected for which the proportion of cash transactions was likely to be high and which had less than 11 employees. The nine

types of retail businesses in Chicago included in the study were (1) bars and clubs, (2) restaurants, fast-food outlets and food stands, (3) barber shops and beauty salons, (4) liquor stores, (5) grocery stores, (6) general merchandise shops, (7) gas stations, (8) laundromats, and (9) pawn shops, currency exchange, and check-cashing services. They found that associations between these urban elements and robbery (violence) within the focal block, in the adjacent blocks and farther away, i.e., the effects were not limited to the immediate block but “spilled over”. The authors found that proximity to retail stores was associated with higher robbery counts. The association with robbery was found in adjacent blocks but the association weakened with increased distance from retail stores. The authors also observed that the crime risks of the block were elevated when a known offender was a resident of the block and, one or more incidents were recorded for drug dealing, prostitution, gambling, and gang-related activities. The crime risk in adjacent blocks was higher when crime attractors (such as places for illegal drug markets or prostitution) and crime generators (such as bus stops, parking places and super markets) were found in them (Bernasco & Block, 2011).

Bowers (2014) studied the influence of risky retail land parcels on the spatial distribution of theft in a large metropolitan area of the UK using 50x50 metre grid cells as the spatial unit of analysis. It was observed that for retail and recreation land use there was a positive non-linear correlation between the frequency of internal thefts in facilities and other commercial land uses and thefts on the street, after controlling for the on-street population (Bowers, 2014). External theft was not found to influence internal thefts for retail and recreation land use, potentially due to perceived lack of opportunities (Bowers, 2014). The study suggests that criminogenic facilities act as “crime radiators” around which crime concentrates and, that as the number of these risky facilities increases, so too does crime. The number of retail land use parcels for external thefts considered in meta-analysis, showed positive but insignificant correlation with thefts.

Favarin (2018) and Vilalta & Fondevila (2019) found that retail shops correlated positively with property crimes and violent crimes respectively. Kim & Hipp (2019), as discussed in Section 3.1.1, used a non-linear statistical model which was not comparable with other studies and hence was excluded from meta-analysis. Clutter et al. (2019) analysed spatial robbery patterns using street segments as a spatial unit of analysis in the BID of Cincinnati for various land uses including Eating places,

Entertainment places, hotels, retail stores, every day stores, grocery stores, pawn shops and Check cashing stores, Salons/barbers, Laundry, Body art parlors, recreation centers, public housing, drug treatment centers and Public libraries (parks, public transit and alcohol outlets are already mentioned earlier). Hotels, everyday stores, recreation centers, public housing and public libraries had a particularly significant positive association with robbery (Clutter et al., 2019). The authors found that street robbery increased whenever additional day stores opened in the BID.

Haberman & Ratcliffe (2015) analysed the influence of ATMs and banks, check-cashing stores, corner stores, drug-treatment centers, fast-food restaurants, pawn shops and public housing on crime. They conducted a temporal analysis for 4 different time periods (early morning - 6.45 A.M. to 9:59 A.M., morning - 10:00 A.M. to 4:29 P.M, afternoon - 4:30 P.M. to 9:14 P.M and night 9.15 P.M. to 6:44A.M) in Philadelphia using census blocks as the spatial unit of analysis. They found an association between patterns of street robbery across all four time periods and the presence of corner stores and fast-food restaurants. Robbery rates in areas with larger numbers of residents and larger concentrated disadvantage was higher in the morning, daytime, and lesser in the evening and night-time. In areas where residential mobility and racial heterogeneity was high, robberies were higher during the evening and late at night (Haberman & Ratcliffe, 2015).

Soohyun O & Yongje (2016) examined 500-ft² grid cells overlaid on Pittsburgh, US and found a positive correlation between retail stores and violent, property and all crimes. However, this study was excluded in the meta-analysis due to the statistical models used not being comparable with the other studies. De Souza & Miller (2012) did not find a correlation with retail stores during the daytime, evening, or night. The authors did find that situational factors played a large role in the occurrence of homicides. They found a positive correlation for convenience stores, bars/clubs, money loan shops and restaurants with violent crime as these places were central to the favela life, but the association was higher during day time and evening and comparatively lower at night (De Souza & Miller, 2012). However, as discussed in section 3.3.5, they used Ordinary least square fixed effect Linear Regression model which is not comparable with other studies and hence this study was excluded from the meta-analysis.

Kim & Wo (2022) analysed seasonal effects of blocks with stores and restaurants and found a non-linear association. Hsu & Miller (2017) studied the effect

of drug-dealing crimes on street segments and intersections in Newark NJ using a matched-case control design. They found that retail facilities (stores, bars, and restaurants) were associated with higher crime on intersections than on street segments. The authors argued that the easy accessibility at intersections generate more crime (Hsu & Miller, 2017). Data from Hsu & Miller (2017) was not included in the meta-analysis due to the statistical models used not being comparable with the other studies.

3.3.6.1 Data synthesis

Studies analyzed retail land use in general or as a combination of various elements of retail land use such as commercial stores, convenience stores, bars/clubs, licensed premises, alcohol stores, fast food joints, restaurants, money loan shops, pawn shops, corner stores, general merchandise shops, gas station stores, laundromats, beauty salons, barbers, personal care shops, and check cashing stores. For each type of retail land use, the aim of the meta-analysis was to estimate the overall effect of that urban element on crime. Hence the effect sizes of each type of retail land uses were combined (see Table 3.14) prior to conducting data synthesis across studies (see Appendix 3-6).

Table 3.14 Predictor Variables-Influence of Retail land use on crime

Authors and Year of Study	Predictor variables for which effect sizes were calculated separately	Data used in meta-analysis
Bowers (2014)	One effect size was calculated for all Retail land parcels and separate effect sizes were calculated for internal and external thefts. As per national land use data base of the UK, Retail land parcels consist of shops, Financial and professional services, Restaurants and cafes and public houses and bars	Effect size for external thefts was used as the study focuses on effects of urban elements on crimes and not internal characteristics of urban elements.
Bernasco & Block (2011)	Effect sizes were calculated separately for general merchandise stores, grocery stores, stores at gas stations, fast food restaurants < 10 employees, Barbers and beauty salons < 10 employees, laundromats, pawn cheques & cheque-cash services, bars, and clubs with <less than 10 employees and Liquor stores	Effect size combined across all Retail land use elements provided in the prior column
Clutter et al., (2019)	Effect sizes were calculated separately for Retail land use, Everyday stores, Grocery stores, eating places/ Restaurants, check cashing & pawn stores, Salons/barbers, Laundry and Drinking places	Effect size combined across all Retail land use elements provided in the prior column (Note: Hotels and ATMs are excluded as they are not a part of Retail land use)
Haberman & Ratcliffe (2015)	Effect sizes were calculated separately for Corner stores, Fast food restaurants, Check cashing stores, pawn shops, bars, and alcohol stores for four different time periods	Effect size combined across all Retail land use elements provided in the prior column
Vilalta & Fondevila, (2019)	Effect sizes were calculated separately for alcohol outlets and No Alcohol stores	Effect size combined across alcohol and no alcohol stores. The effect size for shopping mall was not included as it has different environment from the Retail land use in the studies included in meta-analysis
Favarin (2018)	Effect sizes were calculated separately for Retail shops (excluding licenced premises), personal care shops and licenced premises	Effect size combined across all Retail land use elements provided in the prior column

The statistics were extracted from the studies and the overall effect size computed where data were comparable (Appendix 3-6). The individual effect sizes within each study across multiple retail elements were combined to arrive at the mean effect size of retail land use (see Appendix 3-6).

3.3.6.2 Results

The individual IRRs, their confidence intervals, and the overall mean effect size, where appropriate were plotted on a forest plot (see Figure 3-7). As seen in the forest plot, the mean effect size for property crimes is low (IRR=1.44) and it is statistically insignificant. Bowers (2014) had a much higher IRR (2.16), more than double compared to the other two studies. This could be due to the difference in retail land use components included in these studies across different geographies.

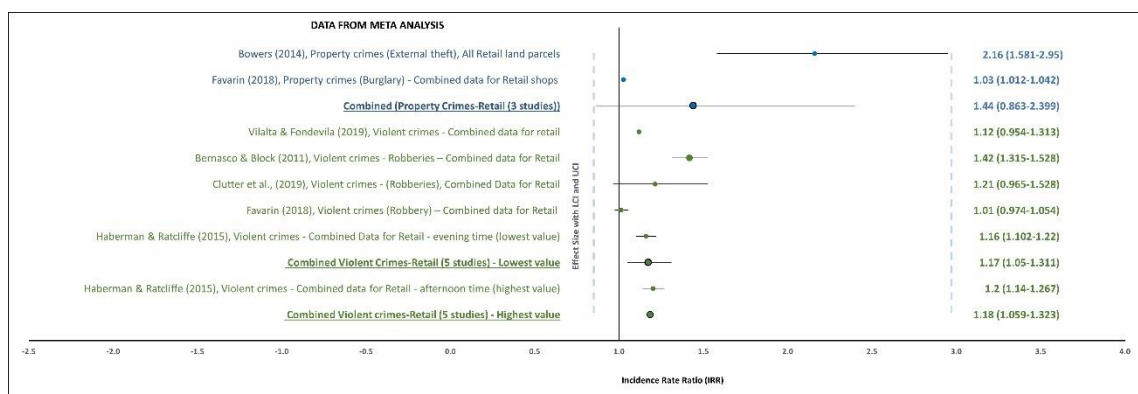


Figure 3-7 Forest plot for Influence of Retail land use on crimes

For violent crimes, six data points were available. Two estimates of the overall effect size were computed due to the way that Haberman & Ratcliffe (2015) reported the results (see above). There was a marginal difference between the least overall mean effect size (IRR = 1.17, significant) and highest overall mean effect size (IRR = 1.18, significant) of retail land use on violent crimes.

Overall, the results of the meta-analysis suggest that despite being defined differently across studies, retail land uses appear to have positive correlation with both property and violent crimes.

3.3.7 Drug treatment centers

A smaller number of studies estimated the effects of the remaining urban features, and hence a shorter reporting format is adopted in the remaining results

sections. Three studies discussed earlier – Clutter et al (2019), Haberman & Ratcliffe (2015) and Groff & Lockwood (2015) – analysed the effect of drug treatment centres on crimes. For violent crimes, Clutter et al. (2019) calculated IRR as 1.1702, Haberman & Ratcliffe (2015) calculated IRR at different times of the day for influence on robbery (1.512–morning, 1.372-daytime 1.537-evening, 1.175–late night), and Groff & Lockwood (2015) calculated IRR as 1.07 for robbery. Property and disorder crimes were analysed by Groff & Lockwood (2014) and the results reported had very similar IRR values – 1.25 and 1.28 respectively. Meta-analysis was conducted (see Appendix 3-7), and the results were presented on a forest plot (see Figure 3-8).

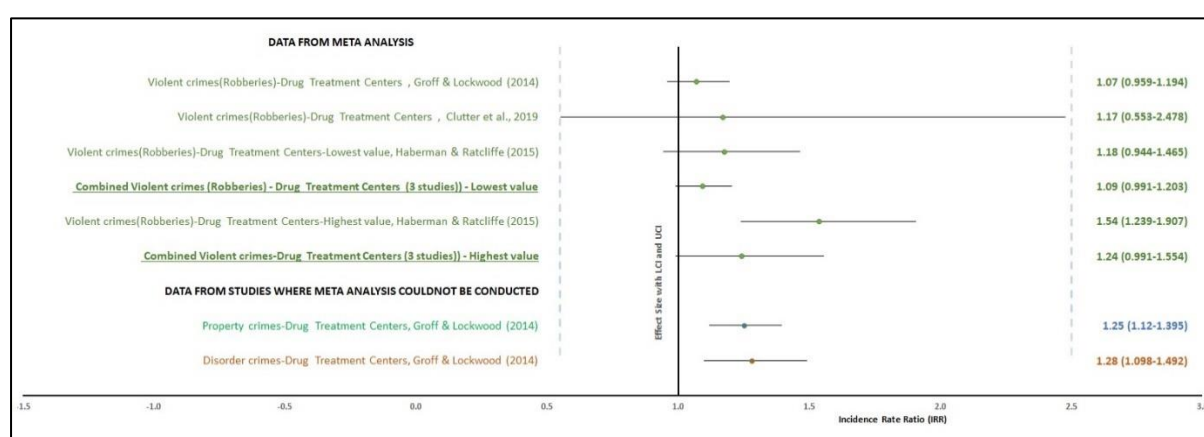


Figure 3-8 Forest plot for Influence of Drug treatment centres on crimes

The overall estimated effect sizes for the association between drug treatment centres and violent crime (least value IRR = 1.09 and highest value IRR = 1.24) were in the positive direction were significant.

3.3.8 Bank Branches and ATMs

Two comparable studies – Favarin (2018) and Haberman & Ratcliffe (2015) – examined the effect of bank branches and ATMs on robberies. The IRR value provided by Favarin (2018) was 1.608. Haberman & Ratcliffe (2015) conducted a temporal analysis to calculate the effect sizes (morning (IRR=1.210), afternoon (IRR=1.344), evening (IRR=1.275) and late night (IRR=1.198)). The variations between effect sizes of these two studies could be due to the differences in geographies of the study areas. Meta-analysis for influence of banks & ATMs on violent crimes (see Appendix 3-8) provided combined lowest effect size IRR=1.23 and highest effect size IRR=1.38 across two studies and both were statistically significant (see Forest plot– Figure 3-9).

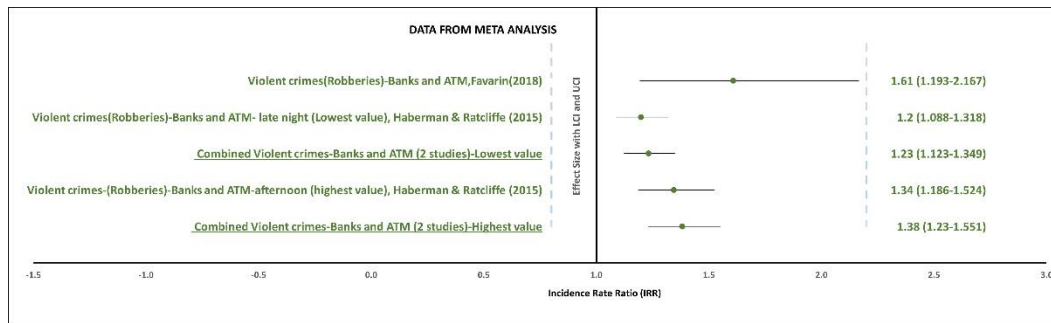


Figure 3-9 Forest plot for Influence of Bank branches and ATMs on crimes

3.3.9 Other urban elements

As was shown in Table 3.1, 40 urban elements were found to have been assessed quantitatively for correlation with crime. Meta-analyses have already been presented for eight of these elements (sections 3.3.1 to 3.3.8). Of the remaining 32 urban elements, six (Hotels, shopping malls, alley ways, windows onto streets, trees, and walkability) were assessed in more than one study, while 26 urban elements were assessed only in one study each. These urban elements are summarised below, along with a summary of how they have been found to correlate with crime (see Table 3.15).

A statistical meta-analysis could not be conducted for the data extracted for hotels, shopping malls, alley ways, trees, and walkability due to these studies using statistical models that were not comparable. Most urban elements in the included studies were associated positively with crime with a few exceptions. Windows onto the street, community and educational buildings within 500m of the centre of street segments, a garden within 150m of the centre of street segments, the percentage of buildings built in past 10 years all had a negative association with crime. Churches on street segments, the greening rate, fire stations and the number of buildings, walls and proportion of grass in the streetscape were not found to be criminogenic.

Table 3.15 Other urban elements and association with crime

Other urban elements found in SR	Number of assessments	Correlation with crimes
Hotels	2	Correlated positively with robbery (Clutter et al., 2019; Kim & Wo, 2022)
Shopping malls	2	Correlated positively with property and violent crimes (Kim & Wo, 2022; Vilalta & Fondevila, 2019)
Alley ways and windows onto street	2	Alleyways Correlated positively with homicide, Windows onto street correlated negatively (Beavon et al., 1994; De Souza & Miller, 2012)
Number of Trees in streetscape	2	Positive association with violent crimes (Deng, 2015) and no influence on property crimes (Xie et al., 2022)
Walkability	2	Positive association with property and violent crimes (Lee & Contreras, 2021; Xie et al., 2022)
Police stations. Total units of public housing on each street segment	1	Police stations correlated positively with robbery. Public housing correlated positively with burglaries and robberies (Favarin, 2018)
Public libraries, recreation centers	1	Correlated positively with robbery (Clutter et al., 2019)
Abandoned buildings, vacant land, mailboxes, parking lots, Churches	1	Churches - Not significantly associated with drug crimes on street segments, but associated significantly at intersections for drug crimes; all others - positive associations with drug crimes (Hsu & Miller, 2017)
Halfway houses	1	Positive correlation with property, violent crimes and disorder crimes (Groff & Lockwood, 2014)
Fire stations	1	Fire stations were not associated with crime (Ratcliffe, 2012)
the number of - sidewalks, streetlamps, enclosure effects, and fences - in the streetscape	1	Positive influence on property crimes (Xie et al., 2022)
the number of - buildings and walls- in streetscape, proportion of grass in the streetscape, and the greening rate	1	No influence on property crimes (Xie et al., 2022)
Physical boundaries between two sides of streets (Land use difference)	1	Positive association with property and violent crimes (Kim & Hipp, 2022)
Number of businesses, Percentage of buildings built in past 10 years, community center and educational building within 500m of center of street segment, garden within 150m of street segment	1	Positive association with property and violent crimes for number of businesses, the rest had negative association (Amram et al., 2024)

Two of the studies shown in Table 3.15 that have not been mentioned in any prior assessment are discussed here. Deng (2015) studied the association between different crime types and (configuration & composition of) trees across Milwaukee, USA using census blocks as a spatial unit and by controlling for socio-economic variables such as age and ethnicity of the population. The findings of the study suggest that configuration as well as the composition of trees with varying heights correlated positively with property crime. Only the density of trees was positively associated with violent crimes, but the effects varied across the city (Deng, 2015). Lee & Contreras (2021) analysed the effects of neighbourhood walkability on property and violent crimes in city blocks of Los Angeles, USA using a negative binomial regression model. The study found a strong influence of walkability with both property and violent crimes (Lee & Contreras, 2021) which was consistent with the crime pattern theory which suggests that the built environment plays a role in influencing criminal activities.

3.4 Discussion

This chapter provides a view of the state of art in terms of the available research and gaps in understanding how urban elements might influence physical crimes at micro spatial units. It also addresses the research gap identified in section 2.2 regarding the lack of systematic reviews analysing the effect sizes of criminogenic urban elements using micro units. This study was conducted at the outset of the PhD with the aim of guiding further research directions. The review provided insights into how urban elements affect crime and addressed the research question “Which urban elements have been quantitatively analyzed for their influence on physical crime using micro spatial units and what is their overall effect on crime?” This review found no literature addressing the influence of people's cyber activities in relation to urban elements in micro-places and their impacts on physical crimes. A total of 40 urban elements were evaluated for their effect on crime across 29 studies, leading to two key findings. First, compared to the other urban elements, places with higher accessibility and connectivity were associated with more crime, including property and violent offences. Second, most (about 75%) of the urban elements examined in this study, were found to be positively associated with more crime, four (10%) were associated negatively with crime and six (15%) had no association with crime.

Meta-analysis could be conducted for only eight urban elements - street network configuration, public transit, parks, schools, alcohol facilities and bars, retail facilities, Drug treatment centers and bank branches & ATMs. The combined effect sizes computed for these eight urban elements were further reviewed to compare how each might affect crime – Figure 3-10 shows a Forest plot of each of the overall estimated effect sizes (from IRR=1.08 to IRR=2.01). For violent crime, the effect of main roads (IRR=2.01) and public transit (IRR=1.98) was found to be relatively higher than for the other urban elements. Public transit was more criminogenic in the surrounding areas, especially for bus stops, tram stops and subways. For property crime, the highest effect size of 1.74 (IRR) was associated with street configuration (using a measure of how likely a street is to be used). This was followed by the combined effect sizes of street configuration using main roads (IRR=1.5). Street segments that are better connected and easily accessible, are travelled frequently, have higher traffic (e.g., main roads) and greater pedestrian flows. Hence these street segments are more susceptible to crime specifically when good quality targets are

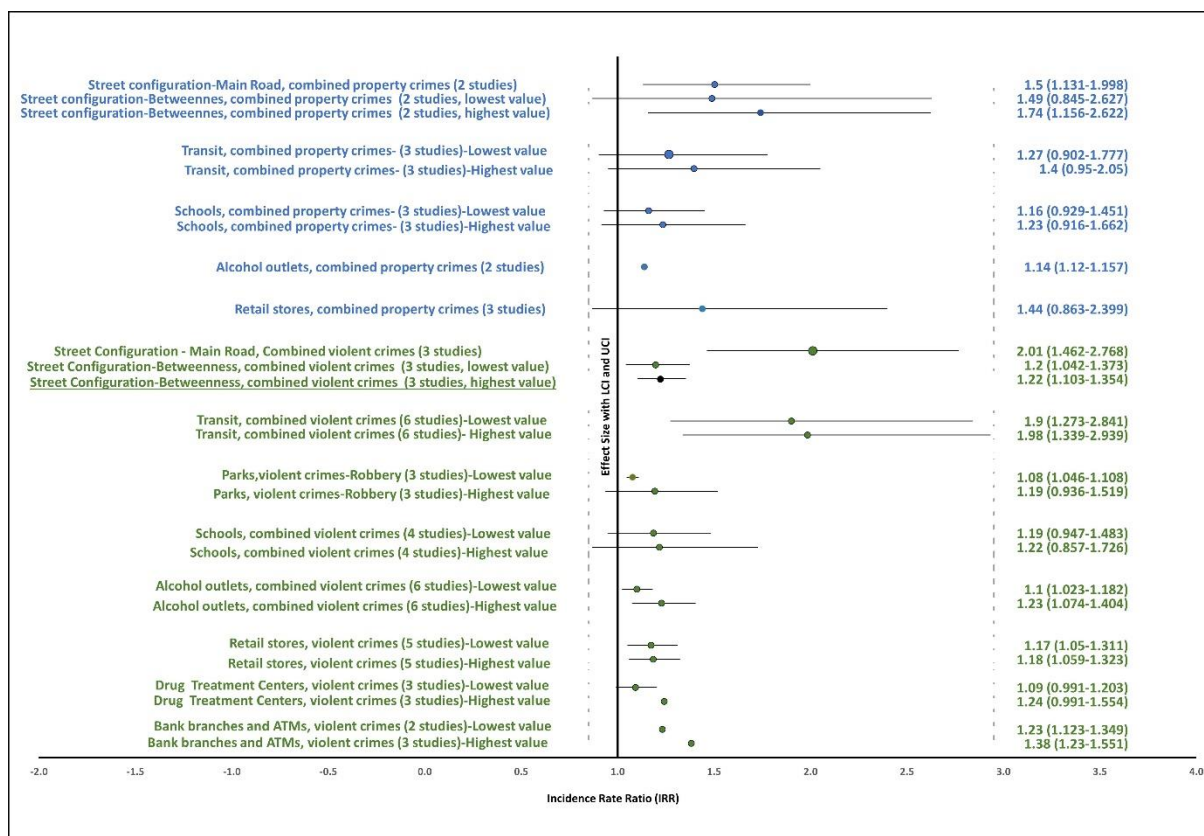


Figure 3-10 Forest plot – summary of the estimated Influence of Urban elements on crime

present on them. These results provide support for crime pattern theory (see Chapter 2, Section 2.1), suggesting that street segments that are busier due to them being within more peoples' activity spaces facilitate more convergences of motivated offenders and vulnerable targets that may lack capable guardianship/ place management generating more crime opportunities (Brantingham & Brantingham, 1995; Davies & Johnson, 2015). The convenience of a road network can influence a criminal's routine activity (see Chapter 2, Section 2.1) and rational choice (see Chapter 2, Section 2.1), both of which play a significant role in an offender's selection of locations to commit a crime.

Different types of facilities exhibited different crime patterns depending on the crime type. The criminogenic effects of schools on property and violent crime were relatively low and insignificant with similar effect sizes that ranged from IRR=1.16 to IRR=1.23. Research has evidenced that places with schools do not have more crimes compared to places without them (Borbely et al., 2023; Macdonald et al., 2018). However, research also suggests that the criminogenic effects depend on factors such as the geography (e.g., some schools in the US are positively associated with serious violent gun crimes (Daniels et al., 2010)), crime type (e.g., research has suggested a

positive significant correlation between schools and disorder crimes (Groff & Lockwood, 2014)), and type of school (public or private; higher education school or primary school as discussed in section 3.3.4). Unfortunately, there were too few studies, which met the inclusion criteria, to test these moderating factors in the current meta-analysis.

For property crime, three urban elements (other than street configuration and schools) were analysed – retail stores, public transit and alcohol outlets. Retail stores and public transit had insignificant effects and alcohol outlets had the lowest significant effect size (IRR=1.14) amongst all urban elements. Offenders might not consider the presence of retail stores as an opportunity for theft due to surveillance / security guards, however retail stores might be associated with internal theft (Bowers, 2014). Research has used various spatial units for assessment and found contradictory evidence for the association between public transit and property crimes. Some studies found a positive association (Kim et al., 2007; Newton et al., 2014c; Pearlstein & Wachs, 1982; Stucky & Smith, 2017; Zahnow & Corcoran, 2019), while some found no association (Ridgeway & Macdonald, 2017a; Wu & Ridgeway, 2021). The correlation may depend on the location of transit stops, the frequency of transport, the number of people taking journeys, the time of the day, the level of accessibility near to transit stops, the spatial unit of analysis and the land-use characteristics of the street segment level (Block & Block, 2000; Ridgeway & Macdonald, 2017b). More people completing journeys and high levels of accessibility near transit stops can result in more theft due to an increase in the availability of opportunities (Newton et al., 2014c; Zahnow & Corcoran, 2019), however, property crimes could be lower as the victim might report the crime after the theft and might not be aware of the location of the offence (Newton et al., 2014b). For alcohol outlets, research suggests that they are associated more with violent and disorder crimes than property crime (Grubestic & Pridemore, 2011; Labrie & Earleywine, 2000; Pridemore & Grubestic, 2013; Quick et al., 2017; Wheeler, 2016).

For violent crime, six urban elements (other than street configuration and schools) were found to be significantly criminogenic – public transit, parks, alcohol outlets, retail stores, drug treatment centres and Bank branches & ATMs. This is supported by many studies, regardless of the spatial units used – parks (Groff & McCord, 2011; Marquet et al., 2019; Taylor et al., 2019), public transit (Pearlstein & Wachs, 1982; Stucky & Smith, 2017; Wu & Ridgeway, 2021), alcohol outlets (Gorman

et al., 2001; Grubestic & Pridemore, 2011; Jennings et al., 2014; Zhu et al., 2004), retail stores (Kinney et al., 1978; Lockwood, 2007), Drug treatment centres (Groff & Lockwood, 2014) and Bank Branches & ATMs (Hsieh & Wang, 2018; Wang & Hsieh, 2021). Research suggests that such facilities place potential offenders and potential targets in close proximity because they concentrate two types of people a) people not familiar with the locality, and b) people with recurring consistent routine activities patterns. These types of facilities spatially structure human activity and in doing so provide crime opportunities, e.g., people might be carrying brand new purchased consumer items, transacting with cash / bank cards or might get into conflict due to stressful situations (such as long queues or effect of alcohol) (Haberman & Kelsay, 2021; Wortley & Townsley, 2016). This could resulting in these facilities being crime generators (Brantingham & Brantingham, 1995; Cohen & Felson, 1979; Weisburd et al., 2012). The lowest significant effect size for violent crime was for parks (IRR=1.08). Research suggests that parks could be crime generators (Groff & Mccord, 2012), however the crime patterns are shaped by multiple features of park and activity generators. Such features include secure fencing, the number of trees clustering, park furniture such as benches, the presence of a playground, the level of maintenance, whether there is lighting after dark, recreation centres, and if there is a main road or transit stop close to a park (Groff & Mccord, 2012; Taylor et al., 2019; Vliet et al., 2021).

The estimates of the influence of urban elements on crime reported here are the effects after controlling for the influence of other socio-economic, socio-demographic, temporal and land use variables, urban features of the study area, and type of crime examined (e.g., robbery rather than assault at alcohol outlets). However, despite the differences in studies, with only a few exceptions, the urban elements examined in this SR that were quantitatively assessed for their influence on crime using micro spatial units, consistently suggest a positive association with one more types of crime. This was regardless of research design, crime type, independent (predictor) variables, the time periods for which data were collected, physical & social characteristics of the study locations, and the statistical models used for quantitative analysis.

The urban elements that had no or a negative correlation with crime were associated with features that increase movement of people and/or increase guardianship - windows onto the street, the greening rate (i.e., the increase in vegetation or green spaces), fire stations, community and educational buildings

including schools (within 500m of the centre of a street segment), the presence of a garden (public or private garden, park, or landscaped area within 150m of the centre of a street segment), the percentage of buildings built in past 10 years, churches on street segments, the number of buildings and walls in the streetscape, and the proportion of grass in the streetscape. However, in the literature reviewed, there was only one assessment of the influence of these urban elements on crime. Hence more data would be required to understand if there is a criminogenic influence of these urban elements at micro places.

The findings from this study can potentially help develop specific targeted measures for crime prevention interventions and urban designs that could limit the criminogenic impacts. For bus stops that were found to be more criminogenic at street intersections than on the street segment itself, redesigning the street layout to reduce congestion or traffic bottlenecks at intersections can make bus stops less vulnerable to criminal activity. Installing CCTV cameras at or near bus stops at intersections can also help monitor criminal activity more effectively. Another targeted measure for crime prevention could be installing physical barriers such as bollards or fences can guide pedestrian movement and prevent loitering or other undesirable behaviours around bus stops. However, as already noted, surprisingly few studies met the inclusion criteria, and hence some caution is necessary, and it may not be appropriate to generalize from the findings for those urban elements discussed for which available data were limited.

Limitations

The results of this review indicate that the literature provides quantitative effect sizes depicting association between urban elements and physical crimes at micro spatial units, however, this is somewhat limited. A comprehensive list of studies were analysed, however, a larger proportion of studies relevant to this line of research where spatial units did not meet the inclusion criteria (65 studies were excluded from the SR as they used large spatial units) were omitted. This is because the aim was to analyse criminogenic effects of urban elements in micro places. Only 29 studies used micro units and were included in the SR. This also suggests that more focus is required for research using micro-spatial units. The number of assessments for an urban element was low (ranged from 1 to 13). Although meta-analysis provided more statistical power with the combined effect sizes and precision of the combined effect

size, the data points that could be combined for comparable studies ranged from only one to eight. In summary, due to the low number of studies for which data could be combined, the results are more suggestive than conclusive.

The studies included in this SR mainly used data directly provided by police departments. Hence, this analysis inherited any limitations that official crime data might have – such as the under reporting of crime that may not represent the entire population. The studies included in meta-analysis also did not consider the impact of any security interventions that could have been implemented but not documented in the studies reviewed. Hence, the results need to be treated with some caution.

Future research

As discussed earlier, 65 studies were excluded as they used large spatial units (see section 3.2.1). Out of the 29 studies that were included in meta-analysis, some studies were further excluded due to non-comparable statistical models. It was somewhat surprising that more studies were not identified that used comparable statistical models. Thirty-two of the 40 urban elements could not be analysed meta-analytically as they were found only in one study or were not comparable. The eight urban elements included in meta-analysis were associated with only two types of crimes – property crimes and violence crimes. More research (including spatio-temporal analysis) is therefore needed to provide comparable analysis of the effects of urban elements on various types of crimes at micro places.

The urban elements for which data were available are those that have existed for some time. However, as discussed in previous chapters, urban elements are now transforming. For example, modern urban elements include digital kiosks, which can be found on many streets. Many traditional urban elements are also being digitally connected (e.g. smart bins facilitate the scheduling of garbage collection), and hence it is important to explore the criminogenic effects of the changing urban elements. No studies were identified in the systematic review that have analysed influence of such elements quantitatively using micro spatial unit of analysis.

Despite using the required search queries, no research was found on the impact of people's cyber activities associated with urban elements in micro-places that influence physical crimes. This could potentially be due to the challenges involved in obtaining such data at the street segment level. With the advancement of digital technological innovations, further research is needed to study the influence of both

cyber and physical capabilities of digital urban elements, and their association with the virtual activities of individuals, governments, and organizations, on physical crimes in micro-places, using quantitative methods.

Technology aided information flows lead to the concept of interconnected public spaces: a mixture of physical and virtual built environments. This concept of connected places (i.e. places where infrastructure in the built environment is connected digitally) also means changes to the activities of people, movement patterns, operations of infrastructure and the way services are consumed by people in urban environments. The crime opportunities provided by the combined digital and physical aspects of the street environment could lead to significant changes to criminal trends across different types of developing urban environments. As such, due to ongoing digital transformations, which are driving changes to streets, there is an urgent need for research to examine if and how crime types are changing, and what is the association between crime and urban elements in the changing street environments, including those that are digital. With this in mind, the next chapter studies how streets are transforming and how these changes might influence the crime and security landscape.

Chapter Four

4 Urban smart infrastructure and security challenges

Countries across the world are going through fundamental, unprecedented and fast-paced transformations of their urban streets, the multiple impacts and challenges of which need to be managed effectively to support sustainable growth (Department for Transport, 2019c). National, regional, and local authorities are currently focussing on flexible, sustainable and adaptable solutions on streets to bring benefits for citizens. City authorities are making efforts jointly with public, private, and academic sectors to improve the performance of city-wide services by investing in smart digital as well as physical infrastructure services. Sustainability initiatives, intended to provide residents with easy access to urban functions (such as jobs, shops, health services), are driving concepts such as the fifteen minute city, twenty minute neighborhood and one minute city (that focuses on the space outside the front door) in countries such as France, UK, Australia, Sweden and Canada (Dunning et al., 2021; O'Sullivan, 2021; Redwood, 2023; Salome & Maassen, 2023). These initiatives combined with technological innovations connect the street infrastructure digitally to gather data about traffic, pedestrians and the environment (Pribyl & Pribyl, 2015). These 'smart street' transformations, connecting street infrastructure to internet, are at an early stage of maturity. However, they can help city authorities with better planning of road space usage, efficient transportation network operations and optimization of mobility services (Barr et al., 2021).

Urban transformations may create new high impact crime opportunities that can be committed remotely due to increasing connectivity (Shaw, 2016; Ahmed & Rani, 2018; Pribyl & Pribyl, 2015; Prislán & Slak, 2018). Chapter 3 analysed how traditional urban elements influence people's routine activities and their interactions with the physical built environment and how these impact upon criminal behaviour. There was insufficient data available in the literature reviewed to analyse the association between urban elements and cybercrime. However, there is awareness that potential vulnerabilities associated with digitally connected elements of street infrastructures, could result in serious cascading impacts in the street environment (Candelieri et al., 2019; Palleti et al., 2021). Cascading impacts are sudden, uncontrolled, and

unforeseen adverse consequences of a cyber-attack that spread beyond the original system attacked; into other inter-connected or inter-related (cyber and/or physical) systems, networks and entities (Kaffenberger & Kopp, 2019; Langer & Kammerstetter, 2015; World Economic Forum, 2016). Cascading impacts that arise from a chain of related security events are known as systemic events (Kaffenberger & Kopp, 2019), and these are changing the nature of cyber-crime and security interventions. The cybersecurity risks specific to smart infrastructure systems, network and services are managed by the individual operators of them (Kaffenberger & Kopp, 2019). However, there are insufficient tools and efforts to strengthen the management of collective cyber risks in connected places across multiple smart infrastructure services (Rehak et al., 2018; Shukla, 2021). This chapter aims to synthesise knowledge on two areas:

- a) The digital capabilities of smart infrastructure, and cybercrimes that may result in the disruption of their services. As discussed in Chapter 2, a narrative review allows the researcher to summarize theories and concepts through the analysis of a broad topic (Baker, 2016). Hence a narrative review was initially conducted to gather current knowledge on the digital capabilities of smart infrastructure.
- b) Cascading impacts in the street environment caused by cyber-attacks on smart urban infrastructure: To explore the current state of research concerning the potential cascading impacts of cyberattacks, two types of literature reviews were considered – systematic and scoping. Systematic literature reviews follow an approach wherein studies are selected using a defined inclusion criteria and data are analyzed from the included studies to address a specific research question in a transparent unbiased way. Scoping reviews (Munn et al., 2018) employ the same approach as systematic reviews but address broader research questions than traditional systematic reviews. As the scope of the literature review was very specific – cascading impacts of cyber-attacks on smart infrastructure, it was decided to conduct a systematic literature review.

The remainder of the chapter proceeds as follows. Section 4.1 is a narrative literature review to provide a background of how smart devices, digital products, connected infrastructure, and smart applications using city-wide datastores interact to create smart services to transform user experiences on streets. It then provides an overview of the changing crime and security landscape. In section 4.2, the smart capabilities of four infrastructure use cases and their cybersecurity challenges are outlined. In section 4.3, the methodology for a systematic literature review of the

cascading impacts of cyber-attacks on the infrastructure use cases is described. Section 4.4 reports the findings for the individual use cases, while Section 4.5 assesses the results across the infrastructure use cases, discusses the findings, and suggests recommendations. Section 4.6 concludes with a discussion of the limitations of the review and the need for a further evidence-based detailed study.

4.1 Background – Digital Transformation of the urban street elements

Digital transformations of urban streets have resulted in a) smart streets with new elements such as digital kiosks, footway robots, and e-scooters, b) changes in the way existing street elements look or operate, including socially distanced benches with charging options, and payments for parking meters through mobile apps, c) an increase in the number of specific digital elements on streets (e.g. the video surveillance market in the UK is expected to grow annually by 4.9% between 2022 and 2027 (Markets and Markets, 2022), d) enhancements to the functionality of street elements such as live schedule displays at bus stops, and e) the phasing out or repurposing of some street such as phone booths and post boxes (CBS News, 2016; Kollwe, 2021; MORE, 2022c).

Innovation and digital transformation are increasingly connecting elements of urban infrastructure to enhance urban services by bringing together different technological advancements (defined in Chapter 1 – introduction and section 4.1) such as Internet of Things (IoT) and Artificial Intelligence (AI). This has allowed local authorities to conduct tests of self-driving vehicles across the cities of the world including the first full-sized self-driving bus in the UK in May 2023 (GOV.UK, 2023b).

Sub-section 4.1.1 below describes the elements of digital street transformations (such as sensors and smart applications) and 4.1.2 considers changes to the crime and security landscape.

4.1.1 Basic elements of Digital Transformations

Digital street transformations are being enabled by data collection and communication between users, sensors, devices, and urban cyber-physical (i.e., physical infrastructure controlled by cyber means) street infrastructure (Park, 2022). Most street elements embed multiple sensors that collect data and initiate a control action through devices known as actuators that produce a physical action in a

controlled manner (Laufs et al., 2020b). Data captured by sensors/devices is occasionally processed by edge computing services which are closer to the source. For example, on-board diagnostic sensors for vehicles provide various functions such as keeping the vehicle in its lane and preventing collisions (Guerrero-Ibáñez et al., 2018). Devices and infrastructure also communicate with each other through networks to enable the sharing and aggregation of data (Hudson-Smith et al., 2021). The data collected from multiple networks may be sent to more centralised cloud gateways (cloud is a term for computing services such as storage, databases, software, servers, processing, and analytics that are delivered through the internet) (Toh, 2020) and aggregated. This connectivity is enabled by technologies such as Ethernet, Fibre optics, satellite, 3G, 4G, and 5G networks (Toh, 2020). Complex city-wide bulk data sets are stored, analysed, and managed using big data technologies (Hudson-Smith et al., 2021). Cloud applications/services subsequently feed responses back through cloud gateways to end user devices (e.g. smart phones) and other user interfaces (e.g. web portals) through an internet gateway (Bauer et al., 2021). The data aggregated from sensors enable real-time monitoring applications. For example, detecting unauthorised intruders in a place using thermal imaging (Pawłowski et al., 2020), counting pedestrians to input into crowd flow management tools (MORE, 2022a), and detecting road conditions for dynamic resource management on streets (e.g. changing lanes, speed limit, bollards, road closures, diversions) (Wolf et al., 2022). For the purposes of illustration, Table 4.1 provides more examples of the data collected by smart sensors and some of their applications.

Table 4.1 Sample applications of sensors on streets

	Types of data collected by sensors	Sample applications	FUNCTIONS					
			Identify and alert for hazard	Match pre-fed information	Provide information to users	Monitoring and analysis	Manage location / service	Crime prevention / detection
Vehicles and pedestrians	Pedestrian count	Analysis of people movements			v	v		
	Location of vehicles and pedestrian footsteps	Smart pedestrian crossings light up (LEDs) based on the location of the pedestrian and/or vehicles, social distancing in Covid-19	v		v			
	Vehicle, vehicle type, card in a vehicle, and licence plate recognition	Automated tolls, total time that a vehicle is parked, access control for vehicles through a barrier, authentication for EV charging, parking fines		v		v	v	v
	On-board vehicle diagnostics	Keeping vehicle in its lane, Cruise control, speed alerts, journey time, fuel indicator, Automatic collision prevention and detection	v		v	v	v	
	Vehicle count	Real-time analysis of types of vehicles and their journeys				v		
	Weigh-in-motion	Measure and record vehicle weights while the vehicle is in motion and check if overweight				v	v	
	Vehicle height	Measure height and alert if too high for underbridge						
	Tracking location of public buses and trams	Information to people waiting at bus stops			v	v	v	
	Vehicle speed	Traffic security and congestion	v		v	v	v	v

Traffic flow and road	Incident detection on motorways	Alert controllers to potential incident, provide information to users for alternate journeys	v		v	v	v	
	Traffic signal	Management of vehicle movement on the roads				v	v	
	Parking space	Availability of parking space, Duration of a parking bay being occupied			v	v	v	
	Pothole detection	Road maintenance alert	v			v	v	
Environment		Manage air quality	v			v	v	
	Water level	Potential warning for floods / rainwater collection / drainage leak	v			v	v	
	Radiation, Electromagnetic levels	Detect leakage over safe limits	v			v	v	
	Soil	Measure soil parameters			v	v	v	
	Light	Streetlights to be Switch on/off				v	v	
	Smoke	Fire alarm	v			v	v	
	Electricity, water, and gas	Measure Consumption, pressure, and flow	v		v	v	v	
	Motion	For a tap to open/ close, streetlight to be brighter, trespassing, pedestrian / vehicle detection	v		v	v	v	v
	Noise	Manage Acoustics, gunshot detection	v			v	v	v

Others	Electricity, water, and gas	Measure Consumption, pressure, and flow	v		v	v	v	
	Level of garbage in a bin	Schedule garbage collection				v	v	
	Wearable sensors	Change in body functions e.g., vulnerable person needing help, fitness measurement, pacemaker for heart, insulin pump for diabetics		v	v	v	v	
	Facial recognition	Identify a “wanted” person		v		v		v
	Thermal	Scan for Covid 19, remote temperature sensing for safety using AI				v	v	
	Mobile app sensors	Contact tracing, contactless payment, access control	v	v	v	v	v	v
	Biometrics	Access control, measure cognitive states, crime prediction based on biometrics such as aggressive expressions or pupil dilation or hand movements, hostile reconnaissance, forensics	v	v	v	v	v	v
	Surveillance	Prevention and detection of crimes, forensics	v			v	v	v

References: (MORE, 2022b)¹, (Toh et al., 2020)², (Karadimas et al., 2016)³, (Hundal et al., 2020)⁴, (Kumar et al., 2021)⁵, (Syrowatka et al., 2021)⁶

Applications of technology-based transformations in connected places have changed the way people go about their day-to-day activities in the built environment. Public transport users can plan multimodal journeys using online journey planners for trains, trams, on-demand taxis (such as Uber service), buses, bicycles, boats, walking as well as micro-mobility and ride sharing options (Ambrosino et al., 2016; Jacobs Karrie, 2022). Journey planners, such as that provided by Transport for London, provide options to select journeys based on user preferences such as mode of transport, renting micro mobility options, cost, walking speed and other parameters (Transport For London, 2023). Interactions with drivers of smart cars through applications such as in-vehicle route guidance systems, radar, speed sensors, global positioning systems and CCTV camera feeds help redirect them to less congested routes, optimise traffic signal timings, informing drivers of any safety messages, such

as diversions to avoid hazards (MORE, 2018). Human wayfinding and route choices are now influenced by a variety of factors such as routes that avoid CCTV cameras, trust in technology automated vehicles and personal choices around using ride sharing options (Millonig & Gartner, 2010). In Germany, pedestrian traffic signals are designed to catch the attention of people gazing at mobile devices while they are on the street (Connected Places Catapult, 2021). In one example, a smartphone app was used to show drivers a real-time map of available on-street parking, the optimal route to the closest available space, and facilitated payment using their mobile phone (Westminster City Council, 2013). These parking services for street users are now being integrated with parking enforcement services, which enables enforcement officers to quickly request the towing of vehicles committing parking offences (SmartCitiesWorld news team, 2023a). In many cities in Russia, Japan and Europe vehicles have inbuilt sensors that automatically alert the authorities if the vehicle is involved in an accident (Öörni & Goulart, 2017). Technologies such as AI and Deep Learning are also used to predict the intention of vehicle drivers, pedestrians, or cyclists; and predict any security or safety concerns (for example by flagging suspicious activity / aggressive behaviour) (Biswal et al., 2021; Toh et al., 2020). In 2021, the electric scooter company *Bird* (in Milwaukee and San Diego) trialled a technology that brings any micro mobility vehicles operating (illegally) on footways to a halt, thus enhancing pedestrian safety (Intelligent Transport, 2021b).

Safety systems have also been built by organizations for robots to deliver parcels/goods by moving at a walking pace on footways while maintaining distance from people and street infrastructure; for example, *Amazon's* delivery robots known as *Scout* delivered customer packages in US cities such as Seattle as a pilot test conducted in 2019, however, the programme was shut down as more improvements were identified (Costelloe, 2019; Stitch World, 2019). Drones, also referred to as Unmanned Aerial Vehicles (UAVs) are cost-effective small pilotless aircraft that use various technologies such as computer vision, artificial intelligence, and object avoidance technology. Apart from having military applications, drones are increasingly used in countries such as China, Ireland, Switzerland, Korea, Saudi Arabia, UAE, Russia, Ukraine, UK, USA, Israel and Ghana to capture real-time video/image, live-stream events, transport goods, detect traffic violations, track people through facial recognition, inspect construction sites, support policing, respond to emergencies, conduct surveillance and even sterilize streets by spraying them with disinfectants

(Ashour et al., 2016; Kunertova, 2023; Sharon, 2021; Management et al., 2015; Shaw, 2016; Vergouw et al., 2016). These rapidly changing urban elements and data driven decision-making have resulted in transformations to the way city authorities operate.

Smart applications in infrastructure, devices or urban sharing platforms (that integrate data sets) aim to provide value-driven connected services to improve the management of physical elements on streets, and optimise urban operations that help to achieve urban sustainability goals (Gracias et al., 2023). When analysed (often using cloud services), the data collected can be aggregated to reveal trends and patterns for decision-making such as improving operations through anomaly detection (e.g. decisions on route diversions based on unexpected traffic jams) (Zhang et al., 2022), understanding customer preferences (e.g. business advertisement decisions based on foot traffic trends) (Savithramma et al., 2022; Toh et al., 2020a), and the provision of new integrated infrastructure services (e.g. scheduling garbage collection based on how full the bins are) across urban streets (Karadimas et al., 2016). Real-time data for multi-modal transportation, including traffic flow and footfall can inform data-driven models valuable for urban planning (Barthélemy et al., 2019). Insights generated from such analysis can also be used to create models for process automation and predictive management using AI and information systems software (Hudson-Smith et al., 2021).

4.1.2 General implications of digital transformations on crime and security

Smart street infrastructure services influence the interactions between people, physical infrastructure, and digital elements of the street ecosystem. While this improves the efficacy of services, they change the crime landscape and can introduce new security risks. In the context of smart streets, the challenge is not just the physical aspects of the street, but also elements of connected cyber spaces that support smart street platforms. Crimes have evolved into four broad categories (Reeh et al., 2019): i) Physical attack with physical impact (e.g. physically destroying sensors for flood detection can prevent early warnings), ii) Physical attack with cyber impact (e.g., tampering with smart electrical meters to prevent them from recording and transmitting the amount of energy used), iii) Cyber-attack with cyber impact (e.g. stealing sensitive data from cloud storage), and iv) Cyber-attack with physical impact (e.g. hacking into traffic light control system to cause accidents, or stealing smart cars by mimicking the electronic key). There could also be blended attacks such as a cyber-enabled physical

attack (e.g. disabling a virtually controlled alarm to allow unauthorised people to attack a facility) or physical-enabled cyber-attack (for example stealing access cards to enter a server room and cause a cyber-attack) (Wyss et al., 2007).

Fast-paced technological innovations and the increased use of technology-dependent solutions can create more vulnerabilities if flaws exist in technological implementations (Frick et al., 2021). Due to the increasing inter-connectivity of street infrastructure (physical objects such as cars, traffic lights, power grids, streetlights, and roads) and devices in people's homes as well as the collection of city-wide data in urban data stores, it is possible for criminal groups to target multiple attractive targets remotely across geographies at the same time; thus maximising the potential rewards with reduced effort as well as reduced risks (Shelden, 2018; Tzezana, 2016). Many users are not aware of how technology can be misused for criminal purpose. Additionally, there is latency in law enforcement solutions for emerging technological solutions. Hence, criminals are able to exploit these vulnerabilities anonymously while encouraging copy-cat attacks that give cyber-criminals plausible deniability (Fruhlinger, 2018). The targets of crime and the modus operandi of criminals are changing as technological innovations are being integrated in urban services. As predicted by Europol in 2015, Critical National Infrastructure (CNI), elderly people, and legal / charity business structures have been increasingly targeted for cyber-attacks potentially due to higher vulnerability or rewards (Europol, 2015; Europol, 2021). Due to the increased smart infrastructure services, Europol also predicted new, sophisticated and complex methods of criminal operations, where the possible emerging threats do not have a historical precedence (Europol, 2015). CNI around the world have been lucrative targets for large-scale cyber-terrorism, espionage and warfare (Martin, 2013). For example, a ransomware attack on the Colonial Pipeline in 2021, resulted in fuel disruption impacts across streets in the USA (Beerman et al., 2023).

Technology enabled transformations of urban elements are redefining the characteristics of places, people's interactions within urban infrastructure services, and even their travel patterns and behaviours. For example, there has been an increased use of digital channels by people and organizations in day-to-day life, including real-time services (Barr et al., 2021; Hino, 2022; Xu & Geng, 2019). As a result, people's behaviours as well as activities are driven by complex physical/virtual interactions with digitally connected devices without them being fully aware of the

safety and security implications. Many smart initiatives include campaigns to encourage a positive change in people's habits (e.g. encouraging walking and cycling rather than vehicular transport), policies to support the changes (e.g. raising the cost of using a car to encourage shared transport) and capture success measures based on people's readiness to change the way they interact with the street environment (Barr et al., 2021). All these initiatives potentially contribute to changes in people's routine activities.

As discussed in Chapter 2, section 2.1, criminal opportunity requires the convergence of three elements represented in Eck's (2010) crime triangle (see Figure 2-1) - offender, target, and place (Eck, 2010). By controlling one or more of the three elements – crime events can be prevented or controlled (Eck, 2010). Recognising that they did not exist in isolation, Eck added three controllers who influence each of these elements in a second layer of the triangle (see Figure 2-1) - handlers (to manage physical/virtual behaviour of an offender), guardians (to protect physical/virtual targets/victims) and place managers (to control activities of a physical/virtual location) (Eck, Clarke, & Guerette, 2007). The absence of any one of these supervisors / controllers increases the opportunity for a crime to be committed. In connected places, the criminal opportunity increases when, for example, one or more of the following occurs: a) unsupervised teenagers could find cyber vulnerabilities and hack into smart transport services (suggests absence of a handler to supervise a potential offender), b) a stealthy malware could be introduced by a cybercriminal to take control of an entire connected system in absence of intrusion detection capability (equivalent to absence of suitable guardianship) and c) operators of smart infrastructure may not have suitable monitoring in place to detect a potential cyber-attack (equivalent to absence of suitable place management).

When the design, rollout and operations of a smart service are outsourced by local authorities to private operators, an additional layer of controller is introduced. That is, the local authorities should have processes in place to assure that the private operators are fulfilling their responsibilities. In the context of IoT enabled smart infrastructure services on smart streets, the security responsibilities of the service operators and their supply-chain are complex and can be mapped in multiple ways (Vakhitova et al., 2016). Here, the place managers monitor the security of the cyberspace whereas the capable guardians could potentially be protecting specific crime targets (Back & Guerette, 2021). As an example, the virtual/physical spaces

may be monitored by place managers through software to generate real-time alerts to identify anomalies in activities and prevent potential incidents. On the other hand, capable guardians could be administering access control measures such as granting or denying permissions for access to services when the user is locked out after multiple failed attempts to login.

Sampson et al. (2010) added a further (third) layer to the crime triangle – super controllers (see Figure 2-1). Super controllers manage the conduct of controllers and support them in order to prevent crime (Sampson et al., 2010). Government departments are one group of super-controllers who can influence place managers by, for example, providing guidelines, standards, policies and regulations for the secure and appropriate usage of services that embed advanced technological innovations. Table 4.2 lists some of the important Government initiatives, regulations, and frameworks intended to help public-private organizations manage the cyber risks of smart infrastructure services in the UK, European Union (EU), and USA. The effective enforcement of crime prevention measures is essential to creating a secure smart environment which reduces crime opportunities. Hence, those using IoT technology, smart products and entities that suffer cyberattacks on their smart systems may face increased scrutiny from regulators, leading to more stringent oversight and potential sanctions (ENISA, 2024; Thales, 2024; U.S.Department of Energy, 2022). Since the guidance and regulatory compliance provided by Governments (super controllers) differs across countries, the focus in Table 4.2 is on the security guidance for smart streets that is used by organizations in the UK. However, a few important initiatives from other countries (such as the USA and EU countries) have been included as they are comparable and referenced in the UK's guidelines (NCSC, 2022b).

The Governments in countries such as the UK, Europe and USA act as super controllers and introduce strategies, legislations, guidelines as well as regulations to secure the cyberspace. The UK Government implemented the first nation-wide cyber security strategy (2016-2021) which was based on a 3D model: Defend, Deter and Develop capabilities to combat cybercrimes (H.M.Government, 2016). The strategy was mapped to the UK's National Cyber security centre (NCSC)'s Capability Assessment Framework (CAF), and had four functions: 1) manage security risk; 2) protect against cyberattacks; 3) minimize the impact of security incidents; and, 4) detect cyber incidents(DCMS-d, 2018). With the advent of smart infrastructure, in

2022, the UK Government published a new national cybersecurity strategy to improve capabilities for managing cyber-resilience smart cross- sector services and to protect core government functions (NCSC, 2022). The European Parliament, to raise the cyber-resilience of CNI, introduced the Network and Information Systems (NIS) regulation in 2018 which made it mandatory for Operators of Essential services and digital service providers in the European Union (EU) to manage cyber risks, and report any cyber-attacks within 72 hours (ENISA, 2017). In 2019, the European Network and Information Security Agency (ENISA) passed new legislation and urged Computer Emergency Response Teams (CERTs) and law enforcement agencies of all EU countries to collaborate to enable effective responses to cybercrime (Hammond, 2012). NIS regulation was updated to NIS2 in 2023 to focus on the security of critical infrastructure and the management of supply chain risks (Muncaster, 2023). The USA did not introduce legislation for cyber-risk management, however, in 2023, the National Institute of Standards and Technology (NIST) updated the guidance for cyber risk assessments to include cyber risk management for smart infrastructure (NIST, 2023).

In 2021, the NCSC supported by DCMS, published cyber security principles for *connected places* (earlier known as smart city/ smart street environment) to support city authorities and their partner organizations to design, build, operate and manage cyber-resilient connected places. In 2022, a National cybersecurity strategy that focuses on managing cybersecurity risks of smart cross-sector services with governance, assurance and strong accountability was published (NCSC, 2022). Recognising some of the risks, the UK's NCSC and DSIT published cybersecurity principles for connected places and secure connected places playbook (DCMS, 2021) to provide integrated guidelines for combined physical, cyber and personnel security of smart services in connected places in a consistent manner (DSIT, 2023; NCSC, 2021b; Shukla et al., 2019). The UK's Center for Protection of National Infrastructure (CPNI) (now NPSA- National Protective Security Authority) provides protective security advice for infrastructure and personnel to businesses and organisations; and also collaborates with NCSC for integrated security standards such as PAS:185 and PAS 185:2023 for connected place security (CPNI, 2022, 2017; *Integrated Security*, 2014; Shukla et al., 2019). This was supported by legislations and regulations for connected places in the UK (National Protective Security Authority (NPSA), 2023); and IoT cybersecurity best practice initiatives in the EU(ENISA, 2024).

Table 4.2 Government interventions for cyber-security risks of connected places and smart infrastructure services

Type of document	Heading	Description	Reference
Strategy	NCSC cybersecurity strategy (2022-2030) by the UK Government	Strategy cyber-resilience of UK's core government functions – "from the delivery of public services to the operation of National Security apparatus".	(NCSC, 2022)
Guidance	Manual for smart streets	To support city authorities "who are conceiving, designing and implementing smart street technologies."	(Transport Technology Forum, 2022)
Guidance	Secure connected places playbook	A comprehensive collection of government guidance on the security of connected places.	(DCMS, 2021)
Guidance	Connected Places Cyber Security Principles	Principles for local authorities to keep in mind to design, build, operate and manage connected places (that include technology, infrastructure, and data-rich environments)	(NCSC, 2021)
Guidance	Connected Places Cyber Security Principles 101	Playbook to guide local authorities across the UK nations when integrating smart cities technologies	(DSIT, 2024a)
Guidance	Designing your connected place to be resilient	Guidance for professionals on how to build a connected place resilient to cyber-attacks or other potential failures	(DCMS, 2022)
Guidance	Good practices for IoT and Smart Infrastructures	An aggregated view of the European Network and Information Security Agency (ENISA) Good Practices for IoT and Smart Infrastructure	(ENISA, 2024)
Guidance	Security-Minded approach to developing Connected Places	Good practices for physical, personnel and process security measures to develop a robust, holistic security-minded approach for connected places	(CPNI, 2022)
Guidance	NIST sp800	Guide for conducting cyber-risk Assessments	(NIST, 2023)
Guidance	UK National Leadership for Risk Identification, Emergency Preparedness, Response and Recovery	Guidance on the roles and responsibilities of UK government and public bodies for different types of emergency response and recovery situations.	(UK Cabinet Office, 2023)
Framework	Capability Assessment framework	Guidance for organisations responsible for vitally important services to implement cyber security & resilience principles, how to apply them and how to measure/assure using Cyber Assessment Framework (CAF).	(NCSC, 2022a)
Framework	Technical Foundations for Smart Connected Systems - NIST	Vision, insights, principles, organizing structures, and voluntary guidance and best practices for smart connected systems in connected places	(National Cybersecurity center of Excellence, 2000)
Framework	The UK Government Resilience Framework	Framework for measures to broaden and strengthen the resilience systems of the UK	(Gov.UK, 2022),
Regulation	Connected Places: related legislation, regulations & guidance	List of Legislations and regulations in support of the guidance contained in PAS 185:2023 - commission by NPSA	(National Protective Security Authority (NPSA), 2023)
Regulation	EU - NIS2 (in force from Jan 2023, to be implemented by Oct 2024)	Update to NIS regulation of 2018 applied in the European Union to respond to the growing threats due to digitalisation and interconnectedness.	(European Commission, 2023a)
Regulation	UK - NIS2 (in force from Jan 2023, to be implemented by Oct 2024)	Update to EU's NIS regulation of 2018 with specific requirements that apply to UK	(Muncaster Phil, 2023)
Regulation	IoT Cybersecurity: regulating the Internet of things	A comprehensive overview of the latest E.U., U.S. and U.K. IoT cybersecurity regulatory initiatives.	(DSIT, 2024b)
Standard	PAS 185:2023	Specifies the principles and requirements for developing and implementing a security-minded approach within a connected place	(CPNI, 2022)

To summarise, for smart IoT-based infrastructure, the super controllers - UK's National Cyber security centre (NCSC), the NIST framework from the USA, and ENISA put the maintenance of sound risk management, cybersecurity-by-design and cyber-resilience by design at the centre of security governance (ENISA, 2024; ICO, 2014; Information Commissioner's Office, 2018; NIST, 2018, 2023; Shukla et al., 2019). However, research and policy interventions usually lag behind technological advancements (Back & Guerette, 2021; Blythe & Johnson, 2021; Ho et al., 2022; Vakhitova et al., 2016). Hence, further research is needed to analyse whether these policy, regulatory and guidance initiatives, which have been rolled out are sufficient to address the increased cyber-attack opportunities associated with smart infrastructure.

4.2 Digital capabilities and cyber risks of smart infrastructure

This section aims to outline in more detail some of the changing capabilities of smart infrastructure and the associated cybersecurity risks. It would not be feasible to analyse the large volume of literature for all forms of smart infrastructure. Hence, a decision was taken to review the smart capabilities of four key smart infrastructure examples. This approach has been used elsewhere by researchers where the aim is to provide targeted information for decision makers (Syrowatka et al., 2021). The sampling strategy employed to identify the use cases was developed to ensure that they covered a broad range of digital capabilities widely used on streets. It also included cross-sector CNI and non-CNI services for connected places to enable the analysis of factors driving differences and similarities across the two. Although examples are provided from various geographies, to analyse specific local issues, there is a focus on smart infrastructure rollouts in the UK. Section 4.2.1 discusses the selection of the smart infrastructure use case samples whereas the remaining sub-sections focus on discussing their smart capabilities and cybersecurity risks.

4.2.1 Sampling of smart infrastructure use cases

The objective of this study was to explore the capabilities of smart infrastructures and the potential associated cybersecurity risks. Hence, it was considered important to include two smart infrastructure use cases – the ones that were used for security and safety. More than half of the world's budgets for the first smart initiatives implemented were spent on public safety and two CNI sectors - energy , and transport (Pasha, 2020). Hence, a decision was made to select additional two infrastructure use cases

from each of these areas. Finally, to enable a forward-thinking view, it was decided that at least one use-case out of the four should focus on street infrastructure being rolled out to replace existing infrastructure based on the UK Government's plans for the next 5-10 years. Based on the above criteria, four use cases were sampled:

- 1) Smart CCTV - Closed-Circuit Television (security through Digital Surveillance),
- 2) Smart lighting columns (public safety at night)
- 3) Smart Electric Vehicle (EV) charging (energy)
- 4) Smart bus stops (transport)

Smart CCTV was selected as it is used widely across cities to prevent, deter, monitor and minimize crime as well as terrorism in public places (Bauer et al., 2021). For example, in China, the country with the highest amount of public surveillance, as of 2022 it was estimated that there were more than 400 million surveillance cameras in the country (Jili, 2022). CCTV usage is on the rise in many countries including US, Japan and UK (estimated 7.3 million public and private CCTVs in the UK since 2022) (Chan, 2023; Clarion Security Systems, 2022).

Lighting columns were selected because a large number of smart lighting columns are found on every urban street across the UK, and there is the potential to retrofit these by connecting them and hosting sensors on them as required (Pardo-Bosch et al., 2022; O'Halloran, 2020; Coolfire, 2018). "*Sharing cities*", a project led by Greater London Authority (GLA) with multiple European countries, has developed and published guidance for replicable digital solutions including surveillance and smart lighting columns with a range of smart infrastructure hosted on it (e.g. CCTV, digital street signs, concealed speakers, e-vehicle charging, flood detection, environment sensors) (GLA, 2020).

EV charging was selected as an infrastructure use case because the UK aspires to be a global leader in the transition from gasoline/diesel vehicles to EVs and EV charging stations (EVCS) that connect the energy infrastructure to the transport infrastructure (Energy Systems Catapult, 2020; HM Government, 2022). To meet net zero targets, the UK Government is planning to roll out at least 300,000 public EV charge points by 2030 and stop the sale of new polluting cars from 2035 (HM Government, 2022; WPI Economics, 2021).

Bus stops were selected because buses are the favourite mode of public transport in the UK (e.g. there are 2 million journeys a day in the UK) and smart

transformation plans for retrofitting bus stops have been prioritised in the UK Government National Bus strategy (Department for Transport, 2020; Department for Transport, 2021). Bus stop environments can potentially host other smart infrastructure (e.g. CCTV, EV charge points and street) to make places safer, usable and effective for passengers (MORE, 2022c). Day-to-day movements, as well as the routine activities of victims and offenders in the built environment are affected by streetlights, public transit options, surveillance systems and driving behaviours. Hence, the selection of the above four use cases is also justified from the perspective of crime pattern theory (section 4.1.2). Table 4.3 summarises the criteria satisfied by the selected use cases.

Table 4.3 Selection of use cases

Criteria	Use case that meets the criteria
A. One use case for each of these areas: public security, public safety, energy, and transport.	CCTV (security through Digital Surveillance), lighting columns (public safety at night), EV charging (energy), bus stops (transport).
B. At least one of the four use cases includes smart infrastructure that was being retrofitted for additional smart capabilities.	Lighting columns and bus stops
C. At least one of the four use cases includes smart infrastructure that hosts other smart infrastructure and/or equipment for public Wi-Fi.	Lighting columns and Bus stops
D. At least one of the four use cases includes smart infrastructure that is being rolled out with an aim to replace any item of the existing street infrastructure to achieve the UK Government's aims for next 5 to 10 years.	EV charging

4.2.2 Smart CCTV

CCTV is widely deployed in public places, both indoors (e.g. at airports, stadiums, shopping malls, railway stations, hospitals, and next to ATMs), and outdoors (e.g. in parks, streets, car parks, and traffic intersections). The key components of a smart CCTV system are the camera, video recorder, cable, monitor and data storage. Multiple CCTV systems with shared components are connected in a network. Multiple such networks provide integrated services such as authentication for people to enter a sensitive location using facial recognition.

CCTV systems are used to deter criminal/antisocial activities, assist law enforcement in maintaining law/order, provide video evidence for post-incident investigation and monitor the conduct of police (Ekblom, 2017). Surveillance image data from CCTV cameras maintained by organizations such as city authorities or

private businesses may be transferred to command and control rooms for monitoring, security and human intervention (Jung & Yoon, 2015). Evaluation research is not unequivocal about whether security is enhanced by CCTV; outcomes appear to depend on factors such as the types of crime committed in the area, population density, existing crime patterns and characteristics of the place in which CCTV was implemented (Gerrell, 2016; Lim et al., 2016; Lim & Wilcox, 2017; Piza et al., 2019a, 2019b; Lee et al., 2019).

Smart CCTV systems include technological advances and smart surveillance capabilities that create value through effective data aggregation that creates meaningful information (Kashef et al., 2021). Smart CCTV system features can include night vision, high resolution, large field of view and thermal imaging (Pawłowski et al., 2020). Video data sources now also include footage collected from drones, wearable body cameras, mobile phone cameras, robotic cameras, and many other innovative methods / devices (Arshad et al., 2022; Wolf et al., 2022; Taylor & Lee, 2019). As shown in Figure 4-1, in a smart CCTV system, the data is usually recorded from one or more of the above mentioned sources, broadcast live and stored in the cloud system through wired or wireless methods (Pawłowski et al., 2020; Ryabchikov et al., 2020). Cloud-based systems provide large storage capacity for remote recording across multiple locations and better processing capabilities (Joh, 2019). Users can interact with CCTV outputs (see Figure 4-1) for manual and automated remote monitoring through multiple application interfaces on many devices (smart phones, remote PCs, remote monitors, or monitoring

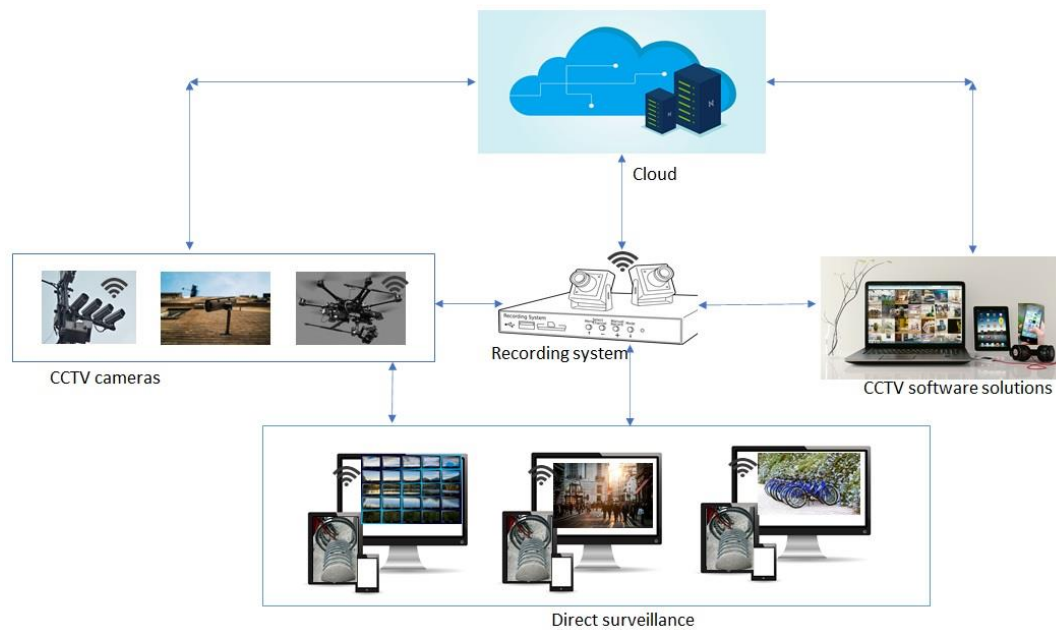


Figure 4-1 Smart CCTV system

centres). For example, security personnel look for abnormal human behaviours at public transit stations through the feed from multiple connected CCTV cameras, police monitor crowd/traffic using real-time surveillance and a bus driver can keep an eye on passengers through on-board CCTV connected to the operator (Barthélemy et al., 2019; Eachus et al., 2013; Lee et al., 2019; Pawłowski et al., 2020).

Real-time monitoring

Technological advances help to automate real-time monitoring to perform tasks that require high speed and precision. Smart surveillance provides flexibility in terms of the types and number of cameras that use sensors to trigger recordings or generate alerts (Hudson-Smith et al., 2021). For example, a recording can be triggered from a specific camera when a human being is detected in the vicinity, and security guards can be alerted when dangerous situations are detected (such as weapons or abandoned objects). Smart surveillance systems improve emergency service response capabilities and the overall resilience of connected places through monitoring, anomaly detection (e.g., when suspicious activities are identified in sensitive areas) that may pose a threat (to people, property, and infrastructure), and automated decision making to trigger quicker pre-determined actions (Lopez-Fuentes et al., 2018; Petrini et al., 2014; Rahman, 2022; Yoon & Chun, 2014). Similarly, the police may be alerted when a

person or vehicle of interest is identified at a particular location using facial or licence plate recognition (Arshad et al., 2022; Lopez-Fuentes et al., 2018; Moellers & Haelterlein, 2013; Ryabchikov et al., 2020).

Intelligent search in recorded footage

Searching through large amounts of recorded CCTV footage is difficult for humans to do manually but can be improved using AI to detect specific objects, reducing the time spent sifting through footage as well as saving network resources (Pawłowski et al., 2020). The software in a video recorder can have built-in intelligence to perform actions on the recorded feed such as quick analysis of long pieces of footage, extraction of footage with a specific licence plate, compression of footage for easy storage, and identification of footage with movement that has a specific date-time stamp (Pawłowski et al., 2020).

Data Analytics

Integrated analytic capacity, reports, and decision-making tools (retrospective, real-time and predictive) have the potential to help organizations become more efficient. For example, risks predicted through video analytics can help with traffic problems, weather forecasting, estimating crowd density, and other services (Andrysiak et al., 2017; Baba et al., 2019; Barthélemy et al., 2019; GLA, 2020; MORE, 2022a; Pawłowski et al., 2020; Vennam et al., 2021; Wolf et al., 2022). The data analytics generated from a collection of video feeds from multiple sources (including social media) can help achieve consensus on a single version of the truth to counter fake information (Lopez-Fuentes et al., 2018; Wolf et al., 2022). Smart CCTV cameras can also be monitored for maintenance and be switched off/on remotely, potentially saving the cost of a site visit to reboot 'crashed' CCTV cameras (Uppal et al., 2023). Surveillance cameras are now able to gather data more accurately for longer periods of time and automate analyses to recognise patterns such as traffic movements, flood detection and the behaviour of people in a crowd (Lopez-Fuentes et al., 2018). This may enable the anticipation of road accidents or antisocial behaviour (Arshad et al., 2022; Heidari et al., 2023).

Key Challenges

Smart technologies are not without limitations. For example, the challenges associated with automated real-time capabilities include false alarms due to automated anomaly detection during surveillance which lack human perception. To reduce the false alarms, the intelligent continuous surveillance is now backed by technological advances such as AI (Arshad et al., 2022; Lopez-Fuentes et al., 2018; Ryabchikov et al., 2020; Jung & Yoon, 2015). Examples of intelligent continuous surveillance include analysing an evolving situation that could turn dangerous and suspicious human behaviour that could lead to a crime event (Arshad et al., 2022; Lopez-Fuentes et al., 2018; Ryabchikov et al., 2020; Jung & Yoon, 2015).

Smart CCTV supports the police by providing smart surveillance applications such as facial recognition, detection of parking rule violation, gunshot detection, and licence plate detection (Rahman, 2022; Laufs & Borrion, 2021). However, poorly developed technology or biased software used for facial recognition have resulted in false arrests, wrongly awarded prison sentences and the violation civil rights.(Hill, 2020; Petkauskas, 2021). For example, in the US in 2016 it was discovered that as a result of a facial recognition system that did not recognise black and Asian people, there have been miscarriages of justice (Eveleth, 2016).

CCTV images may not provide reliable photographic evidence in criminal investigations (Irshad et al., 2021). With the availability of AI tools, it is possible to manipulate the integrity and authenticity of a live or recorded feed, thus making it difficult to distinguish between real and fake media (Khan et al., 2020; Nabi et al., 2022). Digital forensics methods that use technologies such as block-chain (a technology that makes it difficult for the CCTV recording to be changed, hacked, or manipulated) and tools to identify deepfakes (to detect whether the video footage or images are fake) are being used to improve the reliability of CCTV images/videos (Khan et al., 2020; Rocha et al., 2011; Nabi et al., 2022). Other mechanisms to improve the trustworthiness of recorded images/videos from CCTV include but are not limited to robust security measures (Tessian Solutions, 2021).

Media hype, disinformation and fake news add to a creeping fear of authoritarianism arising from a concern that state actors are monitoring citizens all the time through smart surveillance (O'Malley & Smith, 2022). In 2017, people voiced their concerns of authoritarianism when the law enforcement in San Diego, USA began

using the CCTV installed on smart lamp posts to resolve crimes without any accountability for the impact it had on the privacy of the citizens (Telka, 2020). Public reaction finally lead to the local councils in San Diego implementing policy and guidelines on the use of surveillance and facial recognition tools, in a way that empowered citizens to participate in the decisions prior to the rollout of these tools (Tech Policy Press, 2020). CCTV cameras in public places has instilled fear of Government exercising social control over people and criminals using the data captured by the CCTV systems to commit crimes (Weinert, 2019). Consequently, large groups of citizens may disagree with smart CCTV systems being installed in the first place, perhaps leading to vandalism (Ryabchikov et al., 2020). As an example, in 2020, CCTV cameras were introduced in Durham (UK) to enforce speed limits and these cameras were vandalised 15 times in 8 months (Durhamradionews, 2021). In this case, the impact of the vandalism was mitigated by an efficient private contractor who acted quickly to replace the cameras (Durhamradionews, 2021). Surveillance tools can also bring a false sense of security and too much dependency on technology can also result in reduced interactions between the police and the community they serve, which can erode the trust-based relationship (Khan et al., 2020). To summarise, key challenges associated with surveillance data collection, storage and analysis are ethical implications, assurance, governance, addressing the perceptions of people and understanding possible misuses (Heidari et al., 2023; Luppicini & So, 2016; Meijer, 2018; Yaacoub et al., 2020).

Cybersecurity risks

Smart CCTV surveillance has provided valuable early insights into the identification of potential security threats in real-world situations. Examples where CCTV was used to reduce an emerging threat include the Boston Marathon bombings in 2013, the London riots in 2011, and the London bombings in 2005 (Rahman, 2022). However, it is possible to gain unauthorised access to CCTV cameras, take control of the affected equipment across the network and affect the integrity of the video data by manipulating it (Blancaflor et al., 2023). Coordinated cyber-attacks could be implemented using compromised CCTV systems to conduct to invade people's privacy (Lee et al., 2019), steal information from home/office networks, leak sensitive audio/video footage, and potentially sell footage on black markets (Chen, 2023; Chris Lewis Group, 2021; Labus, 2022). Assembled sensitive information can be used to steal identities, stalk people and manipulate CCTV footage to alter criminal cases(Labus, 2022). Cyber-

attackers could also preprogramme CCTV systems to ensure that images are blurred, key functionality are disabled (e.g. gun detection) and recording could be interrupted selectively (Costin, 2016).

Law enforcement agencies that rely on smart CCTV footage for investigations may find their efforts hindered if cyberattacks result in lost or tampered evidence. Reports of cyber-attacks on smart CCTV systems have resulted in the partial erosion of public trust in surveillance systems (Clim et al., 2023; Gianluca, 2016). Some question whether the cameras can be operated in a way that security and privacy are not compromised (Clim et al., 2023; Gianluca, 2016). The surveillance cameras if hacked, can also serve as an entry point for attackers to gain access to broader network resources for further lucrative attacks in connected places. The costs associated with responding to a cyberattack, such as forensic investigations, system repairs, and potential fines, can be significant, leading to financial losses for affected organizations.

There is a need for robust security measures, such as encryption and secure network communication, to mitigate these threats (Costin, 2016). The UK Government introduced the Surveillance Camera Code of Practice under the Protection of Freedoms Act 2012 (PoFA) (Information Commissioner's Office, 2018; ICO, 2014). Globally, institutions need to have a clear cybersecurity framework and policies to inform the public about the use of CCTV in public and commercial spaces (Kim et al., 2020). The demand for, and the technologies used to conduct surveillance are on the rise, however, the expansion needs to assess social and cyber risks, and demand a more effective strategy for national security (Hino, 2022; Rahman, 2022).

4.2.3 Smart Lighting columns

Historically, the function of lighting columns has been to increase illumination on streets when it is dark to improve visibility and consequently facilitate traffic flow, prevent accidents, and create a safe environment (Cho et al., 2019; Steinbach, Perkins, Thompson, et al., 2015). In theory, streetlights can also play a role in security during the hours of darkness by preventing crime, discouraging anti-social behaviour, and reducing the fear of crime (Farrington & Welsh, 2002; Painter & Farrington, 1999). Street lighting may increase the number of public places that can be used safely at night and encourage social control by increasing the number of people who socialise at night and consequently provide informal surveillance (Hyde, 2014; O'Malley &

Smith, 2022). However, research findings concerning the effects of streetlights on crime and road accidents are mixed (Steinbach et al., 2015; Mihale-Wilson et al., 2019). Moreover, lighting columns consume a large percentage (up to 40%) of a city's energy consumption (Chief Digital Officer for London, 2018; Kingson, 2021). Consequently, in recent years, many cities have retrofitted street lights with Light Emitting Diode (LED) bulbs and solar powered bulbs to save energy consumption, reduce carbon emissions, increase bulb life span, lower maintenance costs and meet sustainability targets (Chief Digital Officer for London, 2018; Hyde, 2014; Jin et al., 2016; Pizzuti et al., 2013).

Smart lamp posts are now equipped with sensors (that can detect ambient light levels, sound, location of the lamp posts, motion), wireless communication devices/networks and controllers to manage the functionalities of an individual lamp as well as a network of LED units (Eakambaram, 2017; Jin et al., 2016). For example, in the City of London, the basic functionality of connected place lighting has involved the automated control of lighting including its brightness (based on ambient light) through a central management system (CMS) since 2018 (Robinson, 2019). Networks of dynamic street lighting systems can be managed over the internet and operators can gain insights for optimisation and energy saving (Beccali et al., 2017; Eakambaram, 2017). The key communications (powerline, broadband and wireless) that enable the digital capabilities of streetlights are summarised in Figure 4.2.

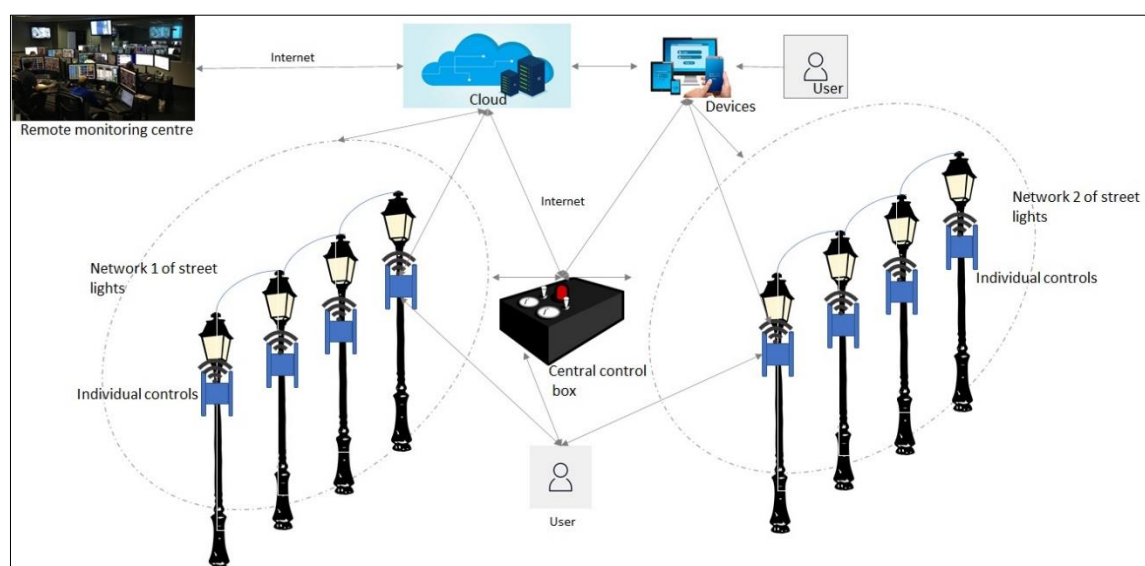


Figure 4-2 Connected place lighting columns

Adaptive lighting

As well as responding to levels of ambient light (Andrysiak et al., 2017; Jin et al., 2016), smart street lights can respond to changes in traffic, diversions, the availability of parking places and even outages in the supply of power (Yilmaz & Uludag, 2021). AI can be used to differentiate between the movement of people, branches/leaves of a tree, cyclists, other vehicles and animals to enable lights to be turned on only for movements associated with people (Omar et al., 2022). Moreover, communication between adjacent streetlights can enable the coordination of lighting levels based on footfall or vehicle traffic (Jin et al., 2016; Omar et al., 2022; Pizzuti et al., 2013). Streetlight network operators can also monitor operations of streetlights remotely via smartphone applications that utilise local and/or remote connectivity through cloud services (Omar et al., 2022; Robinson, 2019).

Monitoring and Data Analytics

Digital communications in the street light system allow central assessment of real-time alerts that flag anomalies (e.g. lamp failure) and can improve maintenance scheduling through web interfaces (Andrysiak et al., 2017; Blackman, 2020; Jin et al., 2016; Omar et al., 2022). Real-time diagnostics and AI assisted predictive data-analytics together enable predictive monitoring (for example, to identify potential accidents), the optimum use of resources (e.g. more resources may be deployed to high accident zones to locate potentially defective lights, or to schedule preventive maintenance) and real-time adaptations. The latter may include automatic illumination adjustment based on the environment or the forecasted traffic rate, while decisions about where to deploy security officers may be optimised based on where incidents are anticipated (Pizzuti et al., 2013; Deepaisarn et al., 2023).

Key Challenges

Lighting columns tend to be positioned at locations on streets where people live, travel, work and participate in activities. They are also safely integrated into the power grid (Blackman, 2020). Consequently, they are ideal for hosting other smart devices and infrastructure. While beneficial, their multi-functionality, and the increasing number of services that they will support, may increase their attractiveness to offenders to conduct cybercrimes and physical crimes (such as vandalism) (DSIT, 2022). While this threat has been recognised, one challenge for the rollout of smart technology such as street lights is the absence of a consistent set of standards, guidelines and policies for operators to use to conduct security risk analysis when transitioning to a connected ecosystem (Alvarez et al., 2022; DSIT, 2022).

Cybersecurity risks

Although there are no known cyber-attacks on smart lampposts that have been reported to disrupt essential services (Stellios et al., 2022a), the smart lighting system acts as an enabler (point-of-entry device) for crimes due to the LED bulbs used being vulnerable to cyberattacks (Franceschi-Bicchierai, 2016; Stellios et al., 2022a, 2022b). A network of smart lighting columns may be an easy target for cybercriminals due to the large number of streetlights in a city, which provide a larger attack surface. Security interventions include continuous monitoring of the network and anomaly detection (Andrysiak et al., 2017). In 2022, researchers show-cased a smart device prototype to monitor anomalies, detect illegal activities (such as theft of lamps, electricity and power cables) and automatic fault registration for repairs (Alba & Linsangan, 2022).

It has been argued that currently, cybersecurity is not prioritised during installation due to a lack of any recorded high-profile attacks on smart streetlights (Stellios et al., 2022a). Current approaches for operating smart streetlight infrastructure are based on public-private partnerships with multiple stakeholders focussing on policy, security standards from vendors, participation from local people, complex accountabilities and networked governance (Offenhuber & Schechtner, 2018; Weinert, 2019). For smart lighting systems, the US Department of Energy and American National Standard Institute (ANSI) have provided cybersecurity strategies, risks, standards and mitigations to protect individual components (Stellios et al., 2022a). The 'Smart street Infrastructure security' report published by the UK Government in 2022 mentions the need for additional measures including risk assessment, updated Publicly Available Specifications (PAS), security rating of the lighting columns, operational oversight by a regulatory authority and future-proofed designs to enhance the physical security of multi-functional street lights (DSIT, 2022). The Department of Science, Innovation and Technology (DSIT) in the UK have suggested that in the future, smart streetlighting systems could look at embedding operational security-by-design within procurement programmes and a governance structure managed by local authorities across stakeholders including the suppliers (DSIT, 2022). The effectiveness of these measures could be measured once these integrated solutions are implemented by local authorities in the UK.

4.2.4 Smart EV charging

Electric vehicles (EV) such as battery electric vehicles, plug-in hybrids, and fuel cell vehicles outperform gasoline powered vehicles in terms of their carbon footprint due to lower greenhouse emissions (Ahmed & Kim, 2017; Holland et al., 2021). Consequently, to meet net zero targets by 2030-2050, many countries are focussing on developing sustainable charging solutions for EVs using electricity from a range of sources (Energy Systems Catapult, 2020; EV Energy Taskforce, 2023; Extrapolate, 2023). The electrification of vehicles in China, USA and Europe (97% of total EVs worldwide) is resulting in the quick growth of EV charging points on streets, parking lots, commercial campuses and private driveways (Extrapolate, 2023).

The basic objective of traditional EV charging stations (EVCS) is to provide convenient facilities, similar to current petrol and diesel stations, for drivers to recharge the batteries of electric or hybrid vehicles (Antoun et al., 2020). The charging infrastructure consists of the EV Battery Management System (BMS), the EVCS, the power grid, an energy management system and the EVCS management system (Pratt & Carroll, 2019). The EVCS has at least one Electric Vehicle Supply Equipment (EVSE), the charging unit (See Figure 4.3) or network of units for EVs, that charges EV batteries at an appropriate rate by communicating with the EV BMS (Chynoweth et al., 2014). Early stand-alone EV charging points were connected to power distribution lines, electricity meters and payment systems, and charging times were setup manually to ensure the reduction of energy use during peak times.

Smart EV charging (see Figure 4.4) include solutions that communicate over internet and networks across EV and EVCSs, between EVs, EVCSs and the Charge Point Operator (CPO) and between the user and application/integrated service providers (Chynoweth et al., 2014; Global, 2023). It is hence important that the charging solutions are interoperable; that is, that various EVCSs, EVs, and their supporting systems can communicate and exchange information without user intervention (Pourmirza & Walker, 2021).

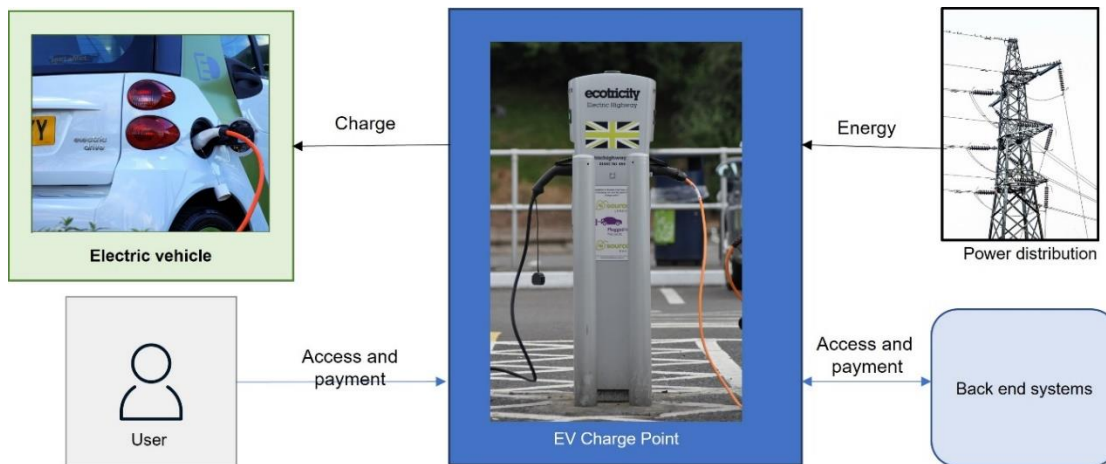


Figure 4-3 EV charging points

EV charging networks consist of cloud-based services (such as data store, EV aggregation – used by grid operators to collectively control the charging of large numbers of EVs, payment processing) and application interfaces for the users (Chynoweth et al., 2014). They manage data between all actors such as users, the CPO, grid control, power distribution lines, EVSE and EVs (Chynoweth et al., 2014). Charging points are being set up as private (e.g. at homes), semi-public (e.g. at workplaces for employees, or shops for shoppers) and public use (e.g. at parking places, at EVCSs and on lighting columns) (Pareek et al., 2020).

Managing demand-supply of the electricity

Power supply and demand are optimised (see Figure 4.4) through bi-directional EV charging. This allows the discharge of batteries, otherwise known as vehicle to grid (or V2G), which supplies unused surplus energy from vehicle batteries to the power grid, as well as grid to vehicle (or G2V) charging (He et al., 2022; Johnson, Berg, et al., 2022). Dynamic demand-supply models used across EVCSs are based on real-time data shared between the EVSE, the EV, and utility companies (Chynoweth et al., 2014; Sygensys, 2022).

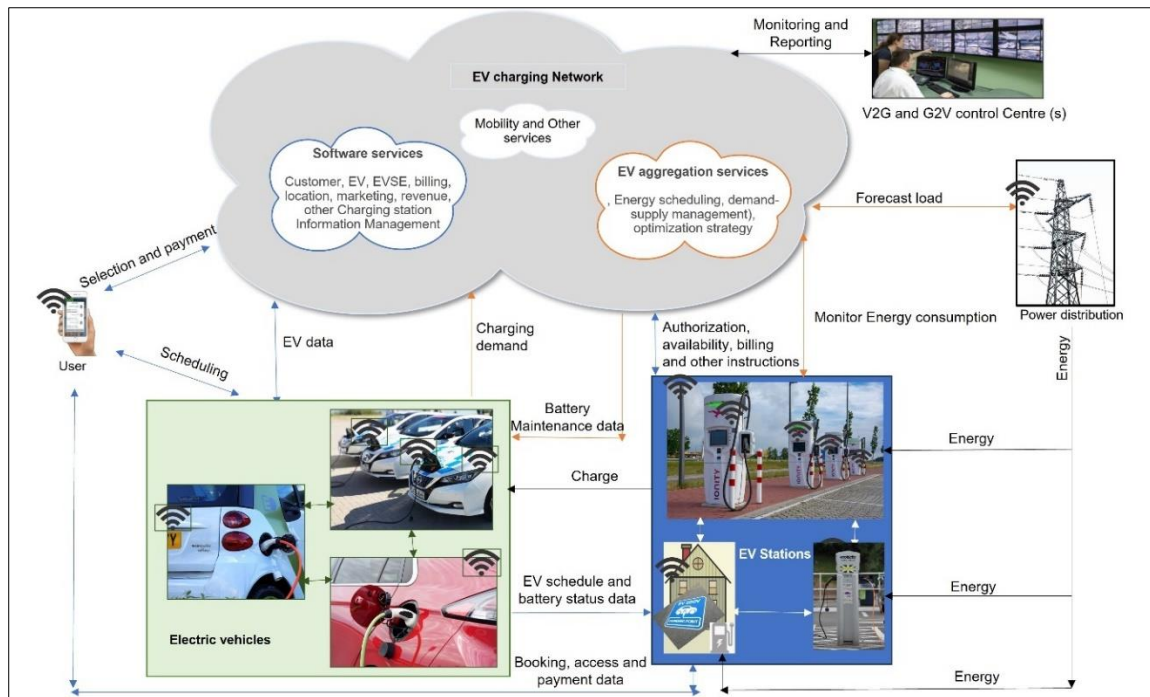


Figure 4-4 Smart EV charging

Services that enable demand-supply management of electricity allow for the optimal scheduling of EV charging to prevent overload (e.g. by allocating charging slots based on availability and vehicle battery data) (Bharatiraja et al., 2017), cost-effective electricity distribution (e.g. customers can be offered cheaper off-peak rates through smartphone applications), the maximization of the use of available grid resources and renewable energy usage options (Sygensys, 2022).

Monitoring, charging applications and Data Analytics

EV charging management software providers ensure management systems for CPO, customers and employees of EVCS through applications, the collection of critical operational data (including charging rates, location of EVCS) and automated monitoring as well as fault detection (Chynoweth et al., 2014; Sygensys, 2022). For example, a software application named *Zapmap* identifies 44,020 public EV charging devices that are available in the UK in July 2023 (DfT, 2023). EV charging users also have access to applications that (for example) provide alerts based on battery status, operational charging locations (integrated with planning for routes), real-time availability of chargers at locations, booking systems and automated licence plate as well as user recognition for easy access (NESCOR, 2015). Charging options, pricing as well as payment systems are digitally automated/integrated with EV user, EVSE used, CPO, and the details of the charging event (Johnson, Berg, et al., 2022;

Sygensys, 2022). The EV charging data and analytics provide dashboard reports for users, CPO, and utility companies (LOTI, 2020a). Data regarding EV charging patterns provide inputs to help improve EV charging systems while monitoring and reducing environmental impacts.

Key challenges

A smart EV charging service may become unavailable due to system failures, such as unavailability of communication systems, power outages, inadequate service from a cloud service provider or a disfunctional software upgrade from a EV manufacturer. Cyber-attacks manipulate demand and supply of energy resulting in physical damage to the transformer, destabilisation of the grid and unexpected costs for consumers (Sygensys, 2022). EV charging network management systems need to avoid overloading infrastructure and to be sufficiently resilient that they can deliver required services despite the disruption of services (Sygensys, 2022). Physical attacks on EVCSS could create very serious challenges. For example, intentionally setting the maximum current to dangerous levels can overheat devices in the network causing fire (Pourmirza & Walker, 2021), and this can also have serious impacts on the integrity of the power grid network (Hamdare et al., 2023).

The design and implementation of charging infrastructure is being improved by technological developments including contactless power transfer, integration with automated driving, and the use of renewable energy sources (Mouli et al., 2017; Pareek et al., 2020). Countries including Germany, Austria, Belgium, Luxembourg, the Netherlands, Poland and the UK have been offering grant schemes to organizations installing and operating smart charging infrastructure to develop better solutions including ultra-fast charging (Chen et al., 2020; SmartCitiesWorld news team, 2023b). The EV charging technology and market are subject to a wide range of regulations that address factors including safety, interoperability, security of supply, and fair and efficient market operation (Sygensys, 2022). To help local authorities in London rollout scalable solutions, Transport for London (TfL), the Greater London Authority, private operators and the London Office of Technology and Innovation (LOTI) have developed common standards for EV charging, frameworks, and a single view of London's EV charge point network (Gov.uk, 2022; LOTI, 2020a). As both generation and demand increases (it is expected to double in 20 years), network constraints such as transmission and distribution capacity, management of the power grid, communication system bandwidth and latency issues will need to be addressed through additional

investment and government policy and regulations. In the UK, the Automated and Electric Vehicles Act (2018) provides the Government with the power to mandate that all EVCS being installed are “smart” (EV Energy Taskforce Working Group 3, 2021).

Cybersecurity risks

In terms of crime targets, offenders could target those engaged in charging events (e.g. EVCS owners, users, operators), the infrastructure (such as EVCS, EVSE), back end services (such as cloud server, third party tools), the power grid, vehicles and/or software applications (ElHussini et al., 2021). For example, smart EV charging infrastructure could enable remote cyber-attacks by flooding the network with fake/unnecessary charging requests to reserve charging slots (also known as jamming), to cause denial of services (Antoun et al., 2020). Attackers might compromise the EVCS systems to take control of its operations. This would enable them to invalidate a user’s access to a EVCS, lock or unlock charging cables, lock drivers out of their vehicles, modify EV charging prices, allow EVs to be charged without payments, compromise billing, steal a user’s identity, steal important energy usage data, leak customer’s private data, and distort consumption patterns to trick EV maintenance companies to potentially cause loss of revenue/blackouts (Acharya, Dvorkin, Pandzic, et al., 2020; IoTNOW, 2022; Jeffay, 2022; Mookerjee, 2022; NESCOR, 2015). The smart EV charging infrastructure is now an attractive target for cyber criminals due to the heightened rewards of being able to impact city power grids, and transport services (Gordon, 2022; Pourmirza & Walker, 2021). Acharya et al (2020) studied the deployment security of 33,320 EVCS in North America and Europe across 22 different vendors. They found weak security practices, a lack of network layer defence, leaving them open to a range of malicious attacks, but also found instances of the EV charging ecosystem being controlled by cybercriminals to deliver malware to other systems (Acharya, Dvorkin, Pandzic, et al., 2020). In 2023, a team of researchers discovered that 455 EVCS were compromised and 57% of these were distributing a malware called Mirai (Acharya, Dvorkin, Pandzic, et al., 2020). In 2016, Mirai malware had infected 1 million IoT devices globally and caused a Distributed Denial of Service (DDoS) attack on major websites (Kolias et al., 2017).

Although there is research on the cybersecurity and resilience risks of smart EV charging, there is limited information about how these are mitigated and governed to limit the impacts to the street ecosystem. In the UK, on the back of EV (Smart Charge Points) legislation in 2020-2021, a regulation was added in 2022 to include

device level requirements, smart features as well as cyber security standards (GOV.UK, 2023a). A framework for cybersecurity and resilience risk management for smart EV charging infrastructure is also outlined in the US NIST guidelines (National Cybersecurity center of Excellence, 2000). The feasibility of meeting the objectives and benefits of smart EV charging solutions depends on the measures taken to manage the cyber-risks of the vulnerabilities in the solution (Pratt & Carroll, 2019). However, there is no literature on whether sufficient measures have been implemented to prevent the cascading impacts of cyber-attacks on EVCS to the power grid.

4.2.5 Smart Bus stops

The basic characteristics of a traditional bus stop environment generally include surface markings for buses, the display of bus timetables and routes, seating for passengers or places for them to wait to board or disembark public buses and connectivity with the footway. The bus stop also provides security to reduce crime, improve social interactions for the elderly and increase perceptions of safety by installing CCTV cameras and lighting (Transport for London, 2017). A smart bus stop provides digital and energy efficient infrastructure. Its environment connects (See Figure 4.5) the transport system, the bus stop infrastructure, road infrastructure, and people through sensors for data collection (such as air pollution, footfall through to traffic monitoring) (Harmony & Gayah, 2017; Kamal et al., 2019). Real time communication systems, cloud storage, control room for monitoring, data analytics, and applications help provide improved integrated services (Harmony & Gayah, 2017; Kamal et al., 2019). As an example of a smart bus stop, Worcester council in the UK has planned bus shelters that include anti-bacterial treatment, integrated CCTV, anti-graffitti gel, interactive screens, cycle and scooter racks, smart lighting, and self-sustainable energy options, such as solar panels, wind turbine energy solutions and sedum green roofs (Intelligent Transport, 2021a).

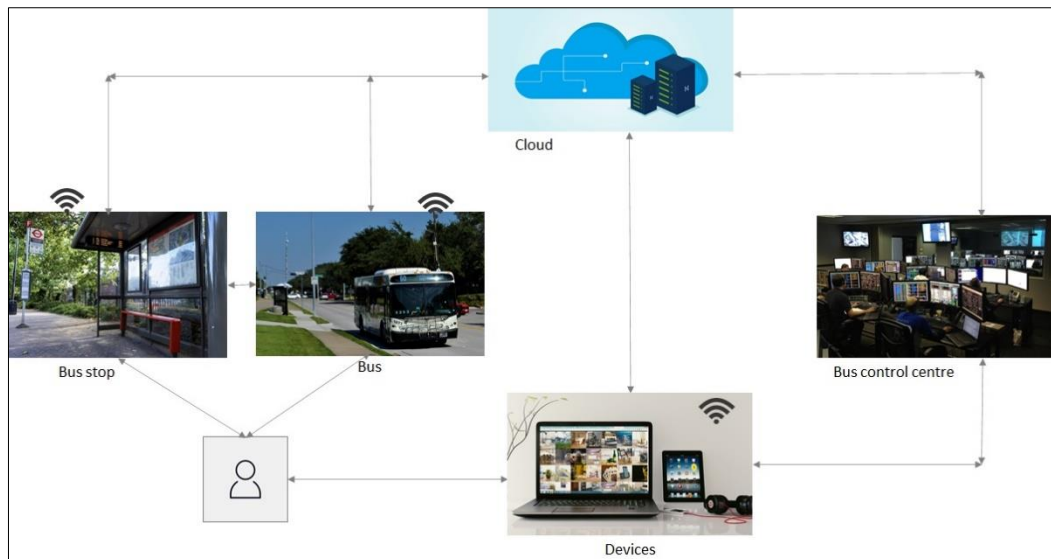


Figure 4-5 Smart bus stops and shelters

Real-time information from the bus

The most common capability of the smart bus stop is the digital display of real-time data about bus schedules, arrivals, delays, route changes, real-time information of buses on interactive maps, and planned or unplanned service alterations. Such information is intended to improve operational efficiency as well as the experience of commuters (Eken & Sayar, 2014; Murad et al., 2018; Nápoles et al., 2020). For example, in 2016 TfL created the “Countdown” service, which provides live bus arrival information for all 19,000 bus stops in London’s network via fixed & mobile web, text messages on mobile phones / messaging apps and 2,500 roadside signs in 2016 (Greater London Authority, 2016). Some smart bus stops also provide additional real-time information from the buses including bus locations, occupancy levels, bus capacity and the availability of free places for wheelchairs and baby strollers (Kumar et al., 2020). Real-time information such as a map that tracks the bus in live traffic, road conditions, weather conditions, journey fares, and service status to help people plan their journeys is also provided through applications to improve ridership (Eken & Sayar, 2014; Nápoles et al., 2020). Drivers also benefit from lights or thermal sensors located at each bus stop on the route, that can sense if a person is waiting at the stop (Kamal et al., 2019).

Additional facilities provided in the bus transit environment

Many facilities are offered at larger bus transit places such as ticket vending, parcel delivery, passenger counting, passenger information, bike rental, heating, smart LEDs, air purifiers, air conditioning, taxi ordering, tourist information, news, charge

points, surveillance, and weather forecasts (Cancelado, n.d.; Intelligent Transport, 2021a; Kamal et al., 2019; Kumar et al., 2020; MORE, 2022a; SmartcitiesWorld news team, 2021; Viegas, 2019). Digital advertising and real-time messages at bus stops – based on the day’s events in the local area – aim to ensure that the information reaches large numbers of people while generating revenue for local authorities (Tu, 2022). For example, displays could convey congratulatory messages to a local team that won a sports event or set expectations about potential route congestion on the day of a football match. Animated content can also be used to capture the attention of passengers to encourage them to follow health and safety advice (Hudson-Smith et al., 2021). In preparation for hosting the World cup in 2026 and the Olympics in 2028, the City of Los Angeles is upgrading 3,000 bus shelters as high-tech mobility hubs with features such as digital adverts, sockets for charging mobile phones, digital lockers and e-scooter docks (He et al., 2022; Tu, 2022).

Smart bus stop design may also aim to increase inclusivity and accessibility for the intelligent transport system by reducing the cognitive demand, providing facilities for the disabled and providing interfaces to people who do not use smart phones (Eken & Sayar, 2014; Kamal et al., 2019; Nápoles et al., 2020). To encourage social inclusivity, some smart bus stops have options for vulnerable customers such as voice interfaces for the elderly (Nápoles et al., 2020), information that can be read using braille and a call button to (for example) hear an automated message about bus schedules, or the option of talking to a human operative (Viegas, 2019). Cities such as Seoul use AI for services such as support with foreign languages for non-local people, and to help visually impaired passengers embark or disembark buses (SmartcitiesWorld news team, 2021). Passengers can also scan Quick Response (QR) codes placed on bus stops using their mobile device to access information (Eken & Sayar, 2014).

On-demand virtual bus stop service

On-demand bus services in many cities (such as Oxford, Hague, Adelaide) provide dynamic data-driven services such as picking up passengers from a ‘virtual bus stop’ close to the location of the passenger, choosing the best route to drop the passengers at their destinations and generating insights for improving the efficacy of the services (Department for Transport, 2019b; SmartcitiesWorld news team, 2021). For example, PickMeUP is the largest network that provides such data-driven on-demand mini-bus services in the UK and complements the public bus services (Department for

Transport, 2019b). Transport for the West Midlands has also initiated the creation of the largest digital on-demand transit service in the UK to connect buses, third-party services, and mobile applications (Smart Cities World news team, 2023).

Monitoring and Data Analytics

Bus stop control centres monitor the bus stop environment, network of buses, quality of service and manage the demand/alterations or closures based on real-time traffic by analysing the data collected from sensors (Ma et al., 2017). Messages are also sent to mobile applications to enable users to view them on smart devices. Data collected from sensors across multiple bus stops enable automatic generations of maintenance alerts to schedule maintenance activities (Kamal et al., 2019). Such big data analytics improves services, increases usage of the public transport, optimises routes and reduces traffic congestion (Yorio et al., 2018).

Key challenges

Accurate real-time information (captured from citizens, devices, infrastructure, and the street ecosystem) on transport network that enables real-time services, attracts more passengers (Alves et al., 2012). However, the transport data collected across the city could be breached and misused by criminals (Nápoles et al., 2020). False information, were it to be displayed on bus stops, could cause traffic jams, overcrowding or influence people's behaviour negatively, including acts of vandalism (Cerrudo, 2015; Ma et al., 2017) – the vandalism of bus stops is already known to occur in areas where there is higher risk of anti-social behaviour and violent crimes (Newton, 2008).

Cybersecurity risks

Checkpoint research team and the Mineta Transportation Institute suggests that ransomware cyber-attacks on the transport sector have increased by 93% over the one-year period June 2021-2022 (Avery, 2023; Careya, 2022). An initial search found examples of cyber-attacks on transport network; no examples were found for cyber-attacks on smart bus stop infrastructure. Cyber-attacks on smart bus networks can impact services such as data processing, on-line ticketing systems, payment systems for bus travel (resulting in revenue loss as well as overwhelming customer support help-lines), the bus operational information provided on mobile applications, a loss of revenue from digital adverts that get disrupted, and the loss of sensitive personal information (Careya, 2022; Cerrudo, 2015; Intelligent Transport, 2021a). Examples of such cyber-attacks on bus networks that occurred during 2021 – 2022 include a ransomware attack against Toronto Transit Commission IT systems, service for smart

cards on a transit company in Quebec-Canada, and scheduling services for Go-Ahead that runs bus services in England (Careya, 2022; Intelligent Transport, 2021a). It is important to manage cyber risks as well as implement a resilience strategy to detect, respond and recover from any cyber-attack as it could impact essential transport services (Katsarov, 2023).

4.3 Cascading impacts of cyber-attacks in connected places

This section discusses the cascading impacts of cyber-attacks on smart infrastructure in connected places and provides the design of a systematic literature review to synthesise knowledge on the same. Cascading failures occur when a disruption in one infrastructure triggers a domino effect across connected, inter-related and inter-dependent infrastructure systems/services. The general focus of smart infrastructure operators is on the direct harm to their services; there is limited understanding of how cascading failures materialise and how they can be mitigated (Chockalingam & Maathuis, 2022; Rajkumar et al., 2024). As mentioned earlier, there is also a lack of ownership for the management of collective cybersecurity risks in a connected place (Rehak et al., 2018; Shukla, 2021), which is now a key focus of the UK NCSC cybersecurity strategy 2022-2030 (NCSC, 2022c). Hence, this section focuses on cascading impacts of cyber-attacks in connected places.

The cascading effects of cyber-attacks on connected place infrastructure can manifest at three levels – first order, second order and tertiary impacts (Macaulay, 2016). *First order cascading impacts* result from a cyber-attack on one node in a network which may lead to a cascade of failures in the entire network and its associated services (Havlin et al., 2010). For example, if a facial recognition system that takes inputs from a CCTV is disrupted due to a cyber-attack on CCTV systems, it can be classified as a first order cascading impact.

Second order cascading impacts are those that originate from first order impacts and that cause a cascade of failures outside the network to services of other connected infrastructure systems (Herrera & Maennel, 2019). In our CCTV example, a second order impact would be a cyber-attack spreading to other connected non-CCTV networks potentially loading ransomware on computers interacting remotely with the facial recognition database.

Tertiary cascading impacts are the effects of the second order impacts (which arose due to the first order impacts) into more inter-dependent entities. In our CCTV

example, the tertiary impacts could be impacts of services that depend on surveillance (e.g. security of a place), financial loss (ransom payment), loss of critical data such as forensic evidence, miscarriages of justice, people losing faith in CCTV systems.

Cascading impacts are not limited to dependent IT systems and networks, they can also affect physical/ cyber-physical interfaces. For example, if a threat actor gains access to a local authority's server network, fake work orders can be sent to contractors - first order impact; the contractors could unknowingly dig over utility pipelines or communication cables based on the fake work order - second order impact and; there could be a possible disruption to utility services, potential impacts to people's safety and financial as well as reputational losses for the local authority and the contractor – tertiary impacts (Cerrudo, 2015; Gianluca, 2016; Stellios et al., 2022a).

In the UK, smart infrastructure is rolled out by local authorities-place managers/controllers who are supported by Government–super controllers and the rollouts often happen in partnership with private firms–also place managers (MORE, 2022b). The local authorities as controllers may not be able to do justice to assurance and governance as all the local authorities are not fully aware of potential criminal misuses, cascading impacts of cyber-attacks and unintended consequences to the connected place ecosystem (Baig et al., 2017; Khatoun & Zeadally, 2017). As a result, the security standards for infrastructure services are driven by the private firms-operators, who are place managers, and accountabilities are complex (Department for Transport, 2019c; Offenhuber & Schechtner, 2018; Weinert, 2019).

In connected places where integrated services operate, one of the security challenges is the identification and management of cascading impacts of cyber-attacks that disrupt people's activities at a larger scale compared to the impacts that are contained within the system attacked (Kaffenberger & Kopp, 2019). Disrupting people's routine activities at scale creates incentives or increases rewards for offenders. A cyber-attack on digitally connected CNI or non-CNI infrastructure services could have society-wide cascading impacts on connected places (Palleti et al., 2021), such as the disruption of public services, a compromise to assets/people's safety, adverse economic/political events or threats to national security (World Economic Forum, 2016). For example, in 2003, the cascading effects of a cyberattack on a communication system resulted in blackouts in the US and Canada (Palleti et al., 2021).

The private operators of connected infrastructure and services focus on preparing for the specific cyber risks associated with the first order cascading impacts for their systems, infrastructure, services and the networks operated by them (Kaffenberger & Kopp, 2019). However, the collective local or regional risks of the first, second and tertiary cascading impacts to other connected infrastructure, services and networks in a connected place is not analysed by the private operators or local authorities (Shukla, 2021). It is consequently important for local authorities to assess the risks of digital services in the connected places that they are building. As controllers, local authorities need to understand the inter-dependencies created by connected infrastructure and integrated services as well as the threat scenarios so that they can make sure that the place managers – operators have a plan of action to reduce the likelihood of severe cascading impacts of cyber-attacks (Langer & Kammerstetter, 2015).

It is challenging to assess whether the security measures in a connected place are proportionate to the criminogenic risks introduced by the smart infrastructure rollouts (Palleti et al., 2021). Barns et al (2016) and Kobie (2015) stated that there are key issues in the governance of smart services which include the lack of understanding of two key elements: a) the specific cyber-attack scenarios that could spread across sectors and disrupt inter-connected integrated services in connected places, and b) how the recovery procedures should be planned in anticipation of such cascading impacts considering that coordination would be required across multiple organizations and services (Barns et al., 2016; Kobie, 2015).

4.3.1 Focus of the systematic literature review

The purpose of the systematic literature review was to explore the current state of research for cascading impacts of cyber-attacks on smart infrastructure in connected places. The research question for this systematic literature review was “In the event of a cyber-attack on smart infrastructure, what are the potential cascading impacts in connected places (or urban street environments)?”. The scope of this systematic literature review was to identify cybercrime scenarios across inter-connected infrastructure services and understand their cascading impacts in connected places for the four use-cases considered in this chapter. The focus was on cyber-crimes and cascading impacts (first order, second order and tertiary) that have already occurred or have been analysed as plausible by researchers. The cascading effects of a cyber-

attack within the components of a single system which can be contained within that system are not in scope of this literature review. This is because the aim is to analyse the cascading impacts in connected places - across systems within and outside the network of connected infrastructure.

4.3.2 Search strategy

A key limitation of the academic literature on topics such as that covered here is that it can be limited, and there is a latency associated with its publication. Moreover, information about on-going and planned smart infrastructure strategies across the world are often to be found in documents published by governments. For this reason, to identify literature the Google scholar search engine was used as it indexes a variety of publications that are not limited to academic literature (Yasin et al., 2020).

After conducting initial test searches and finding a balance between being comprehensive and maintaining relevance, the keywords shown in Table 4.4 were selected. These were intended to capture the specific details of use-case considered, smart features of the infrastructure, and threat scenarios/cascading failures caused by a cyber-attack. Searches were limited to the last decade to ensure that the results were relevant to current initiatives for connected places, crime, and security.

Table 4.4 Search Keywords for literature review

Search Topic	Search keywords		Search Topic	Search keywords		Search Topic	Search keywords
CCTV	CCTV, surveillance, "video surveillance", "smart camera", "Internet of Surveillance things"					Cyber-attacks with cascading impacts	"attack effect", "cascading impact", "ripple effect", "attack scenario", "cyber attack", "cyber-attack", "cyber threat analysis", "failure scenario", "security assessment", "security analysis", "threat analysis", "threat assessment", "cybersecurity threat", "cybersecurity risk", "Cybersecurity assessment", "reports of attacks", "risk analysis"
Lighting columns	"lighting column", "streetlight", "lamp post", "lighting poles", "smart lighting network"	+	Smart features	smart, connected, intelligent	+		
EV charging	"EV charging", "Electric vehicle charging", EVSE, EVCS, "EV charging ecosystem"						
Bus stops	"bus stop", "bus shelter", "bus stand", "bus transit"						

The searches were initially conducted in March 2023 and then updated from 27 March 2024 to 5 April 2024. The search was carried out separately for each of the infrastructure use cases (see Appendix 4-1). Six articles (grey literature – 3 news reports, 2 blog articles, 1- private company report) that detailed incidents of cyber-attack on smart infrastructure were suggested by the researcher's professional network and included in the study (See Appendix 4-2). All search results and grey literature were reviewed against the inclusion criteria (discussed in Section 4.3.3). Backward and forward searches were carried out once relevant studies that met the inclusion criteria were identified. Forward searches were conducted by identifying

highly cited studies and studies that cited them. Backward searches were conducted by reviewing the bibliography of identified articles for other studies that might be relevant.

4.3.3 Criteria for screening of search Results

Studies were screened using the following inclusion criteria:

- a. The studies must be in English for practical reasons
- b. Studies must be published in the past ten years to ensure that the information is relevant.
- c. Studies must be available in full (not in part or incomplete).
- d. Studies must be peer reviewed or from a credible public/private/Government source (hence, dissertations were excluded). An exception was made for real-world incidents, real-world vulnerabilities, and real-world demonstrations - media reports were included for these.
- e. Studies must discuss cybercrime threat scenarios and/or its impacts for one or more of the four infrastructures sampled as use cases in connected places. Studies that discuss cyber-attacks on non-infrastructure elements (such as cyber-attacks to conduct corporate espionage, credit card theft or personal data theft from an urban data store) were excluded.
- f. Studies must describe cyber-attacks that have already occurred or shown as plausible by researchers.
- g. Studies must describe first order, second order and/or tertiary impacts of cyber-attacks.
- h. Studies were excluded if they discussed cyber threats for smart infrastructure within private premises, buildings, and homes, or if the cyber-attacks did not directly impact any of the four use cases considered here.

4.3.4 Data extraction

The following information was extracted from included studies:

- a) Author and year of study
- b) City and country associated with the cyber-attack scenario (where the studies did not include an incident/ demonstration/ experiment in a specified location, the city and country associated with the author was used). This data was

collected to understand which countries are actively researching or dealing with cascading impacts of cyber-attacks on smart infrastructure.

- c) Type of cyber-attack scenario (see below)
- d) Cascading impacts of cyber-attack (see below)
- e) Type of evidence (see below)

Type of cyber-attack scenario

Initially, the descriptions of the cyber-attacks were extracted as articulated in the studies reviewed. A thematic analysis (Ayres, 2007; Thomas & Harden, 2008) – a method where qualitative data is organised into key patterns/ themes, was conducted. Based on this thematic analysis, two unique forms (or high-level themes) of cyber-attack scenarios were identified-

- a) Disruptions to smart service availability (e.g. DDos attack), and
- b) Tampering with the functionality of smart infrastructure, disrupting the integrity of the associated data or smart service (e.g. blurring CCTV footage).

Cascading impacts of cyber attacks

The threat scenarios/incidents and their cascading impacts from each study, and a set of unique cascading impacts for each scenario identified using a thematic analysis were extracted. The cascading impacts were then classified as first order, second order and tertiary impacts. As discussed in the beginning of this section, cascading impacts can be caused by various types of systemic cyber events (a chain of multiple security events affecting multiple entities) (Kaffenberger & Kopp, 2019). The cyber-attack scenarios and the three levels of cascading impacts were synthesised and coded as representing one of five types of systemic cyber events (Kaffenberger & Kopp, 2019), as follows:

- a) one incident at massive scale,
- b) multiple incidents at massive scale,
- c) multiple incidents at small scale over time,
- d) multiple incidents simultaneously, and
- e) a few scenarios close to simultaneous succession

Types of evidence

The included studies provided cybercrime scenarios that may or may not have occurred. Hence, the research method used in each study was assessed using a hierarchy of evidence (see Table 4.5), based on the approach taken by Blythe & Johnson (2021). The aim of this was to assess the quality of evidence to understand the plausibility of the cyber-attack scenarios discussed in each article (Blythe & Johnson, 2021). For example, a live hack demonstrated by researchers in the real-world would be considered more plausible than a desktop simulation.

Table 4.5 Hierarchy of evidence – systematic review of cascading impacts of a cyber-attack

Type of evidence	Description
Real-world Incident	A cyber-attack that has already occurred in real-world
Demonstration by hacking systems in real-world	Demonstration of cyber-attack on live real-world systems. Usually, such cyber-attacks do not cause harm as the purpose is to create awareness
Real-world vulnerability	Analysis of a vulnerability discovered in the real-world that would allow cyber-attackers to exploit the systems
Experiment in a test-bed	Demonstration of cyber-attack and its impacts in a physical test-bed created for the purpose of conducting an experiment
Proof-of-concept	A model created as desktop exercise (with or without full source code) using real-world data to demonstrate a cyber-attack for a specific use case
Simulation	Demonstration of cyber-attack and its impacts in a computer-generated simulation
Expert speculative	A cyber-threat derived by a group of experts using standard threat or risk assessment models/methods (example STRIDE threat model, where STRIDE stands for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege)
Author speculative	A cyber-threat derived by a desktop exercise using standard threat or risk assessment models/methods and/or literature review

Table 4.5 was used to review the mechanism through which the cybercrimes and cascading impacts were realised. If the evidence was speculative, it was mapped to more cyber-attack scenarios where evidence was not speculative to determine its plausibility.

4.4 Results – Systematic literature review

4.4.1 Summary of search results

After the removal of studies not in English and duplicates, a total of 601 studies (208 CCTV+160 for lighting columns+209 for EV charging +24 for bus stops) were identified across the four use cases. Of these, 51 studies (6 for CCTV, 3 for lighting columns,

and 42 for EV charging, but none for bus stops) met the inclusion criteria (see Figure 4.6 for screening outputs).

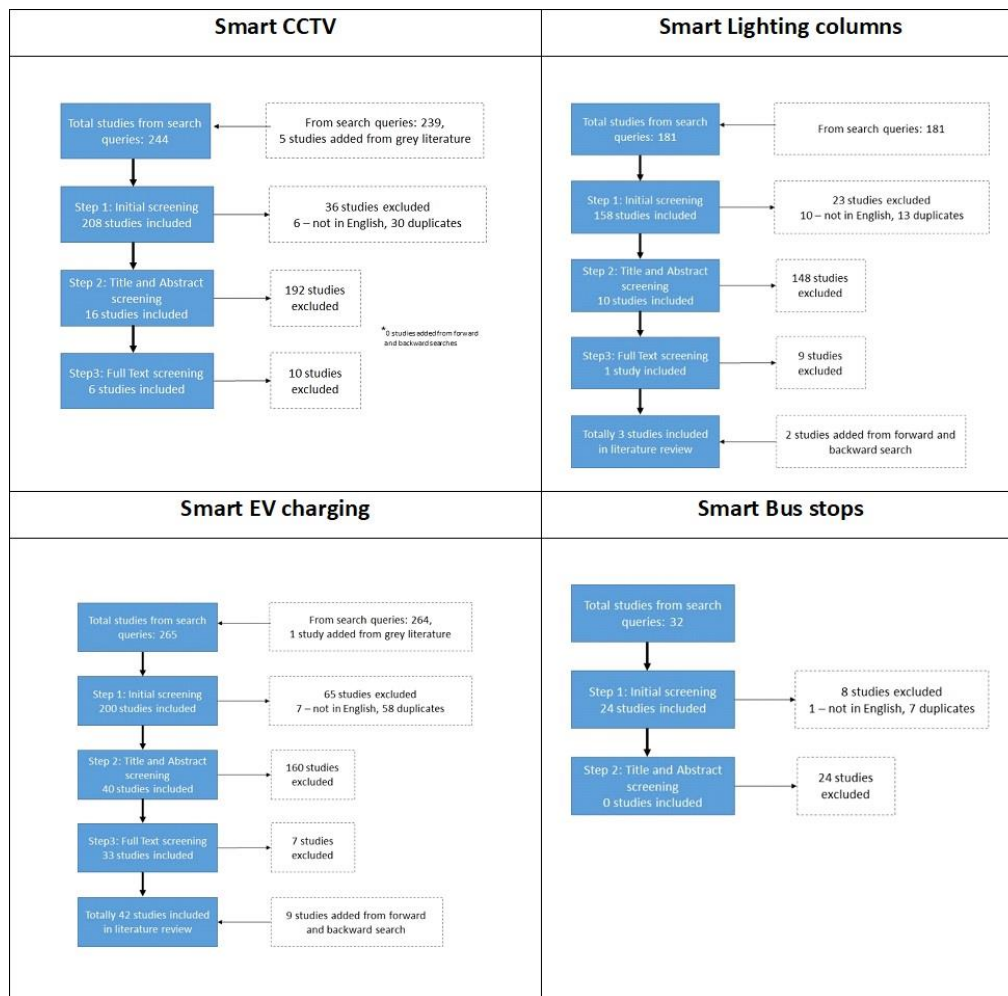


Figure 4-6 Prisma chart

The search results were verified through a peer review process (described in Chapter 3) to avert personal biases in selection of the studies and ensure accuracy. Inter-rater reliability i.e. the degree of agreement (Virta, 2013) among reviewers was assessed. Any disagreements were planned to be resolved through discussion and by consulting a third researcher if necessary. Prevalence-Adjusted Bias-Adjusted Kappa (PABAK) statistic was selected to give a measure for (IRR), to determine the consistency of the ratings. The PABAK measure of 0.9 indicated that there was high agreement between the reviewers (Tang et al., 2011).

Before detailing the content of the studies reviewed, it is worth making three general observations. First, no cyber-attack incidents or threat scenarios that resulted in cascading effects were found for smart bus stops and smart lighting columns. While authors could have speculated on these threats, no studies that did so were identified.

For smart lighting networks (for public lighting, smart buildings, and stadiums), cyber-attack scenarios were found wherein a cyber attacker could gain entry to connected networks through smart lights. Considering that these vulnerabilities also exist in the connected lights of smart lighting columns, these studies were included. Second, compared to smart EV charging, the total number of studies meeting the inclusion criteria were very low for smart CCTV and smart lighting columns. Third, only eight EV charging threat scenarios described all three types (first order, second order and tertiary) of cascading impacts (see Table 4.6). For smart CCTV and smart lighting, a limited number of first order impacts were found, but second order and tertiary impacts were not discussed.

Table 4.6 Number of cascading impacts found in studies included in systematic literature review

Smart infrastructure use cases	Number of studies that met inclusion criteria	Number of unique cyber-attack scenarios that met inclusion criteria	Number of cascading impacts		
			First order Impacts only	First and second order Impacts	First, second and Tertiary Impacts
CCTV	6	5	5	None	None
Lights	3	3	3	None	None
EV charging	42	8	2	4	2
Bus stop	None	None	None	None	None

4.4.2 Smart CCTV

As shown in Table 4.7, four of the six included studies for smart CCTV discussed cyber-attack incidents that had occurred, one discussed a real-world vulnerability, and one study discussed a demonstration of a live hack scenario. Five studies described the impacts of denial-of-service attacks on a CCTV network while one described the impacts of cyber-attackers tampering with the functionality of the CCTV network.

Table 4.7 Studies for smart streetlight included in systematic literature review to study cascading impacts of cyber-attacks

Studies (6)	City/country	Type of evidence	Types of cyber-attacks	
			Denial of service	Tampering with functionality
(Bitnik, 2014)	London, UK	Demonstration by hacking systems in real-world	v	
(Hackread, 2017)	Washington DC, USA	Real-world Incident	v	
(Rahman, 2022), (Hussain, 2016)	Singapore	Real-world Incident	v	
(Smith, 2018)	Japan	Real-world Incident	v	
(Tenable Research, 2018)	Not available	Real-world vulnerability		v

Five unique cyber-attack scenarios causing four types of systemic cyber events were found, although discussions of cascading impacts were limited or none-existent. The five scenarios are discussed below.

One incident at massive scale

Hackread (2017) reported an incident from Jan 2017 where 70% of the CCTV cameras in public spaces in Washington DC were remotely taken out of service – and a ransom demand issued – 8 days before the President’s inauguration (Hackread, 2017). This incident posed a national security threat. To reduce the threat, and to avoid paying the ransom, a major reinstallation of the CCTV cameras’ software was completed prior to the inauguration (Hackread, 2017).

In a different example, Hussain (2016) and Rahman (2022) discussed an incident where a hostile actor hacked into a police-operated CCTV system during the 2015 Southeast Asian games in Singapore to disrupt “live” critical security monitoring (Rahman, 2022). This issue could have resulted in a major security incident in a high profile international event, however, the risk was mitigated by technicians who worked urgently to recover the CCTV functionality (Hussain, 2016).

Multiple incidents at small scale simultaneously

Smith (2018) published smart CCTV security incident from May 2018 in Japan Times wherein more than 60 CCTV cameras were hijacked and defaced at key waterways and a fish market (Smith, 2018). As a consequence of the hackers compromising surveillance, the Japanese local government institutions were unable to monitor the levels of their waterways (Smith, 2018).

Multiple incidents at small scale over time

Tenable Research (2018) discovered a critical zero day vulnerability named Peekaboo in the Network Video Recorder software of a private organization called NUUO potentially impacting approximately 100,000 installations world-wide (Tenable Research, 2018). In a proof of concept study, the researchers demonstrated that a hostile actor could take over multiple connected cameras across cities (Tenable Research, 2018). The vulnerability could have allowed attackers to remotely view feeds, disconnect the feeds and manipulate live/recorded footage (Tenable Research, 2018). If exploited, the vulnerability could have resulted in high impacts due to the worldwide integration of these video surveillance systems (Tenable Research, 2018).

Few incidents close to simultaneous succession

Bitnik (2014) reported a real-world demonstration of a cyber-attack on CCTV surveillance systems, three days prior to the London Olympics in 2012 (Bitnik, 2014). With the aim of increasing awareness of smart CCTV vulnerabilities, without causing harm, the researchers took control of CCTV cameras in twenty locations including public places (Bitnik, 2014). They replaced the real-time footage with a temporary invitation to play chess (Bitnik, 2014). Only one impact was stated where a shop owner disconnected his surveillance camera possibly due to loss of faith in the system (Bitnik, 2014), but the demonstration showed the potential for significant disruption.

4.4.3 Smart Lighting columns

Three studies that met the inclusion criteria discussed plausible threats to smart lighting networks, although no real-world incidents were described. One study described a disruption to services whereas two described impacts that would result from cyber-attackers tampering with the functionality of smart lighting networks (see Table 4.8).

Table 4.8 Studies for smart streetlight included in systematic literature review to study cascading impacts of cyber-attacks

Studies (3)	City/country	Type of evidence	Types of cyber-attacks	
			Denial of service	Tampering with functionality
(Andrysiak et al., 2017).	Poland	Experiment in a testbed		v
(Ronen & Shamir, 2016)	Israel*	Experiment in a testbed		v
(Stellios et al., 2022a)	Greece*	Threat model	v	

* The city and country associated with the author

Three cyber-attack scenarios causing three types of systemic events were described, and are summarised below, but again the discussion of cascading impacts was limited.

One incident at massive scale

Stellios et al.(2022a) discussed a cyber-attack threat scenario where multiple lights in a public place such as a sports stadium could be switched off by a malicious actor, which could cause panic, injuries and even deaths (Stellios et al., 2022a). If a hostile actor chooses to cause further harm, it could be achieved by remotely triggering a fire alarm accessible from the same network and switching off the lights during the evacuation process (Stellios et al., 2022a).

Multiple incidents at small scale over time

Andrysiak et al (2017) discussed a cyber-attack scenario for a connected street light network wherein an attacker could change the settings of lights in the entire network; they may reduce the brightness of the lights or switch them on/off selectively during the night or day. In this case, the only potential impacts speculated by the author were a possible increase in crime, accidents at street intersections and the loss of operator revenue (Andrysiak et al., 2017: p. 13). The authors conducted predictive analysis for such a scenario to occur, proposed a solution to detect it and conducted an experiment to demonstrate that the solution was feasible.

Few incidents close to simultaneous succession

Using an experimental setup of a smart light system in a controlled environment, Ronen et al (2016) demonstrated that the frequency of LED lighting in Philips Lux and LimitlessLED can be manipulated to ranges that can potentially “*induce seizures in people suffering from photosensitive epilepsy*”; in the same way that rapidly flashing video games can do so (Ronen & Shamir, 2016: p. 5).

In another experiment, the authors created a covert channel (i.e. communication channel used by a piece of malware) to hack into data from a smart lighting network system of a highly secure office building. One smart lamp (Philips HUE system lightbulbs) was remotely infected and the malware spread across the office network enabling the authors to control a large number of smart lighting systems from a distance of over 100 meters using only cheap and readily available equipment (Ronen & Shamir, 2016). This scenario is relevant to streetlights as local authorities have begun switching over to LED streetlights (some of which could potentially be from Philips) for energy efficiency benefits as discussed in Section 4.2.3. It is possible that this vulnerability might be secured, however, the scenario increases awareness of potential similar risks.

4.3.4 Smart EV charging

Out of the 42 studies identified (see Table 4.9), seven studies described only denial of service attacks; 16 studies described only the impacts of tampering with EV charging functionality, whereas 22 studies described the impacts of both types of cyber-attacks. The included studies were associated with 21 countries.

Table 4.9 Studies for smart EV charging included in systematic literature review to study cascading impacts of cyber-attacks

Studies (42)	City/country	Type of evidence	Types of cyber-attacks	
			Denial of service	Tampering with functionality
(Skarga-Bandurova et al., 2022) <i>Used 2 types of evidence</i>	Russia, UK	Real-world Incidents	v	v
	UK*, Germany*	Author speculative	v	v
(Malik & Anwar, 2022) <i>Used 2 types of evidence</i>	Russia, UK	Real-world Incidents	v	v
	USA* and Pakistan*	Simulation		v
(Plaka et al., 2023) <i>Used 2 types of evidence</i>	Russia, UK	Real-world incidents	v	v
	UK*	Author speculative	v	
(Jeffay, 2022)	Russia	Real-world Incident	v	
(Carey, 2022)	Isle of Wight, UK	Real-world Incident		v
(David, 2022)	Isle of Wight, UK	Real-world Incident		v
(Sarieddine et al., 2024) <i>Used 2 types of evidence</i>	USA*, Canada*	Real-world vulnerability and simulation	v	v
(Reeh et al., 2019)	USA	Experiment in a testbed	v	v
(Elmo et al., 2023) <i>Used 2 types of Evidence</i>	Wright State University, USA	Experiment in a testbed and Proof-of-concept	v	
(Köhler et al., 2022)	UK*, Switzerland*	Experiment in a testbed	v	
(Nasr et al., 2023)	Canada*, USA*	Experiment in a testbed		v
(Acharya, Dvorkin, & Karri, 2020)	Manhattan, NY, USA	Proof-of-concept	v	v
(Sarieddine et al., 2023)	USA*, Canada*	Proof-of-concept and Simulation	v	v
(Basnet & Ali, 2021)	USA*	Simulation	v	v
(ElHussini et al., 2021)	Canada*, Qatar*	Simulation	v	v
(Nasr et al., 2022)	Canada*, USA*, UAE*	Simulation	v	v
(Nisar et al., 2022)	Australia*	Simulation	v	
(Kabir et al., 2021)	Canada*	Simulation		v
(Khan et al., 2021)	Toronto, Canada	Simulation		v
(Ghafouri et al., 2022)	Australia	Simulation		v

(Phiri et al., 2022)	Zambia*	Simulation		v
(Sayed et al., 2021)	Canada*	Simulation		v
(Soykan et al., 2021)	Turkey	Simulation		v
(Wei & Lin, 2023)	China	Simulation		v
(Carroll et al., 2022)	USA	Expert speculative	v	v
(Harnett et al., 2018)	USA	Expert speculative	v	v
(Johnson, Anderson, et al., 2022)	USA	Expert speculative	v	v
(Sygensys for National Grid ESO, 2022)	UK	Expert speculative	v	v
(NESCOR, 2015)	USA	Expert speculative	v	v
(Johnson, Berg, et al., 2022)	USA	Expert speculative	v	
(Acharya, Dvorkin, Pandzic, et al., 2020)	USA and Croasia*	Author speculative	v	v
(Alcaraz et al., 2023)	Spain*	Author speculative	v	v
(Antoun et al., 2020)	Canada*	Author speculative	v	v
(Brighente et al., 2023)	Italy*, USA*, Singapore*	Author speculative	v	v
(Garofalaki et al., 2022)	Greece*, UK*	Author speculative	v	v
(Girdhar et al., 2021)	USA* and South Korea*	Author speculative	v	v
(Girdhar et al., 2022)	USA* and South Korea*	Author speculative	v	v
(Hamdare et al., 2023)	UK*, Jordan*, China*, Spain*, India*	Author speculative	v	v
(Conti et al., 2022)	Italy*, USA*	Author speculative		v
(Gumrukcu et al., 2022)	Germany*	Author speculative		v
(Metere et al., 2022)	UK*	Author speculative		v
(Pourmirza & Walker, 2021)	UK	Author speculative		v

* The city and country associated with the author

Given the larger number of studies involved, Table 4.10 provides a summary of the types of evidence employed across them. It should be noted that six studies (Elmo et.al, 2023; Sariaeddine et.al, 2023; Sariaeddine et. al, 2024; Plaka et. al, 2023; Malik & Anwar, 2022; and Skarga-Bandurova et al, 2022) used more than one type of evidence and hence appear in more than one cell of Table 4.10.

Table 4.10 Hierarchy of evidence found in systematic review of cascading impacts of cyber-attacks on smart infrastructure.

Type of Evidence	Number of studies	Studies
Real-world Incident	6	(Carey, 2022; David, 2022; Jeffay, 2022; Plaka et al., 2023; Skarga-Bandurova et al., 2022; Malik & Anwar, 2022)
Real-world vulnerability	1	(Sariaeddine et al., 2024)
Demonstration by hacking systems in real-world	None	
Experiment in a test-bed	4	(Köhler et al., 2022; Nasr et al., 2023; Reeh et al., 2019; Elmo et al., 2023)
Proof-of-concept	3	(Acharya, Dvorkin, & Karri, 2020; Elmo et al., 2023; Sariaeddine et al., 2023)
Simulation	14	(Basnet & Ali, 2021; ElHussini et al., 2021; Ghafouri et al., 2022; Kabir et al., 2021; Khan et al., 2021; Nasr et al., 2022; Nisar et al., 2022; Phiri et al., 2022; Sayed et al., 2021; Soykan et al., 2021; Wei & Lin, 2023; Malik & Anwar, 2022; Sariaeddine et al., 2023, 2024)
Expert speculative	6	(Carroll et al., 2022; Harnett et al., 2018; Johnson, Anderson, et al., 2022; Johnson, Berg, et al., 2022; NESCOR, 2015; Sygensys for National Grid ESO, 2022)
Author speculative	14	(Acharya, Dvorkin, Pandzic, et al., 2020; Alcaraz et al., 2023; Antoun et al., 2020; Brighente et al., 2023; Conti et al., 2022; Garofalaki et al., 2022; Girdhar et al., 2021, 2022; Gumrukcu et al., 2022; Hamdare et al., 2023; Metere et al., 2022; Pourmirza & Walker, 2021; Plaka et al., 2023; Skarga-Bandurova et al., 2022)

Eight unique cyber-attack scenarios were identified for all five types of systemic cyber events. The cyber-attack scenarios described in the 14 studies that used ‘author speculative’ evidence, were also described in other studies where more robust evidence was provided (e.g. real-world incidents). Consequently, each of the cyber-attacks discussed below can be considered plausible. Expert speculative scenarios were created collaboratively by private industry practitioners, technical experts, asset owners and academics in workshops using Government guidance. These scenarios are considered plausible as they are created by a group of cross-disciplinary experts using standard threat assessment methods to provide inputs to the industry for “risk assessment, planning, procurement, training, tabletop exercises and security testing”.

Two cyber-attack scenarios provided all three types of cascading impacts, four scenarios provided first as well as second order impacts whereas two scenarios provided only first order impacts.

One incident at massive scale

29 studies described a cyber-attack scenario where a cyber attacker could cause an EVCS to change the rules of power consumption flow established with the power grid. The first order impact could be on EV infrastructure, the second order impact on the local distribution power grid infrastructure, which can then spread to multiple other power grids causing tertiary cascading impacts (see Figure 4.7).

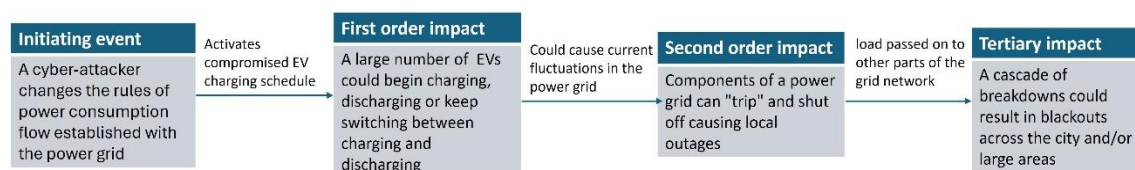


Figure 4-7 Smart EV charging cascading impacts - One incident at massive scale

Hostile actors could aim to disrupt the power grid through cyber-attacks on EVCS. They could initially compromise EVCS servers, or EV charging smartphone applications to tamper with charging schedules (Acharya, Dvorkin, Pandzic, et al., 2020; ElHussini et al., 2021; Pourmirza & Walker, 2021; Sarieddine et al., 2023; Soykan et al., 2021), and create a network of infected EVs as well as EVCS also known as botnet, that the cyber-attackers could control (Acharya, Dvorkin, Pandzic, et al., 2020; Khan et al., 2021; Wei & Lin, 2023). According to Acharya et al. (2020a,b), it is also possible for hostile actors to conduct reconnaissance using publicly available data to establish the capacity of power grids and their consumption patterns to plan cyber-attacks (Acharya, Dvorkin, & Karri, 2020; Acharya, Dvorkin, Pandzic, et al., 2020). They could also hack the customer databases and make unauthorized changes to charging rules by sending fake messages to consumers (Acharya, Dvorkin, & Karri, 2020; Acharya, Dvorkin, Pandzic, et al., 2020; ElHussini et al., 2021; Girdhar et al., 2021; Khan et al., 2021; Pourmirza & Walker, 2021; Reeh et al., 2019; Soykan et al., 2021; Sygensys for National Grid ESO, 2022) or by hacking into the translation protocols used by EVSEs and EVs (NESCOR, 2015; Skarga-Bandurova et al., 2022).

These types of cyber-attacks could cause surges in electricity demand, surges in power supply or continuously switch between high demand and high supply. Surges in electricity could be caused by a large number of EVs charging at the same time

across multiple EVSE creating a sudden surge in demand during peak times when the grid has fewer reserves to supply the extra demand (Acharya, Dvorkin, & Karri, 2020; Acharya, Dvorkin, Pandzic, et al., 2020; ElHussini et al., 2021; Garofalaki et al., 2022; Ghafouri et al., 2022; Girdhar et al., 2022; Gumrukcu et al., 2022; Harnett et al., 2018; Johnson, Anderson, et al., 2022; Khan et al., 2021; Metere et al., 2022; Nasr et al., 2022, 2023; NESCOR, 2015; Pourmirza & Walker, 2021; Reeh et al., 2019; Sarieddine et al., 2023; Sayed et al., 2021; Skarga-Bandurova et al., 2022; Soykan et al., 2021; Sygensys for National Grid ESO, 2022; Wei & Lin, 2023). Surges in supply could be caused by making the EVCS and EVs reverse the flow of electricity also known as discharging (Alcaraz et al., 2023; Antoun et al., 2020; ElHussini et al., 2021; Garofalaki et al., 2022; Ghafouri et al., 2022; Gumrukcu et al., 2022; Hamdare et al., 2023; J. Johnson, Anderson, et al., 2022; Metere et al., 2022; Nasr et al., 2023, 2022; Sarieddine et al., 2023; Skarga-Bandurova et al., 2022). A switching attack could cause many EVs to continuously switch between charging and discharging leading to EVs alternating between increased power injection and increased power demand (ElHussini et al., 2021; Ghafouri et al., 2022; Girdhar et al., 2021; Kabir et al., 2021; Nasr et al., 2022, 2023; Sarieddine et al., 2024; Sayed et al., 2021; Skarga-Bandurova et al., 2022; Sygensys for National Grid ESO, 2022).

These types of first order impact would cause a high degree of fluctuations/ imbalance in the power grid that it is not designed to handle. This would invoke safety measures similar to tripping a circuit breaker resulting in the failures in the power distribution transformer thus resulting in local outages – a second order impact (Acharya, Dvorkin, & Karri, 2020; Acharya, Dvorkin, Pandzic, et al., 2020; Alcaraz et al., 2023; Girdhar et al., 2021, 2022; Khan et al., 2021; NESCOR, 2015; Reeh et al., 2019; Soykan et al., 2021; Sygensys for National Grid ESO, 2022). Such local outages would cause the load of the grid to be diverted to other grids in the network, however, these could also cause cascading failures across multiple power grids potentially resulting in a blackout across the city – a tertiary impact (Acharya, Dvorkin, & Karri, 2020; Acharya, Dvorkin, Pandzic, et al., 2020; Alcaraz et al., 2023; Antoun et al., 2020; ElHussini et al., 2021; Garofalaki et al., 2022; Ghafouri et al., 2022; Girdhar et al., 2021, 2022; Gumrukcu et al., 2022; Hamdare et al., 2023; Harnett et al., 2018; Johnson, Anderson, et al., 2022; Kabir et al., 2021; Khan et al., 2021; Metere et al., 2022; Nasr et al., 2022, 2023; NESCOR, 2015; Phiri et al., 2022; Pourmirza & Walker, 2021; Reeh et al., 2019; Sarieddine et al., 2023, 2024; Sayed et al., 2021; Soykan et

al., 2021; Sygensys for National Grid ESO, 2022; Wei & Lin, 2023). Also discussed was the possibility that there could be potential erratic behaviour when the grid is restarted making recovery difficult (Sygensys for National Grid ESO, 2022). No other examples of tertiary impacts were identified.

Multiple incidents at massive scale

26 studies described how threat actors could conduct DDoS attacks (see Figure 4.8) at a massive scale across smart EVSE, thus overloading the charger and causing cascading impacts. Some of the key methods included jamming attacks to overload the charger by sending multiple unnecessary traffic to the EVSE, (Antoun et al., 2020; Basnet & Ali, 2021; Brighente et al., 2023; Elmo et al., 2023; Garofalaki et al., 2022; Girdhar et al., 2022; Hamdare et al., 2023; Johnson, Anderson, et al., 2022; Nasr et al., 2022; Plaka et al., 2023) injection of a signal into the charging cable to interfere with the EV charging process (Köhler et al., 2022) rejecting legitimate charging requests from users, (Girdhar et al., 2021, 2022; Nisar et al., 2022; Sarieddine et al., 2024) and the disruption of 5G services (Basnet & Ali, 2021).

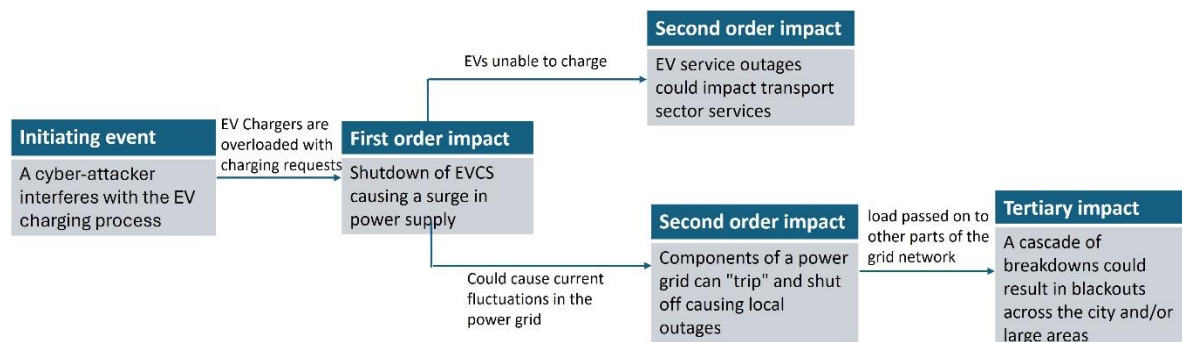


Figure 4-8 Smart EV charging cascading impacts - Multiple incidents at massive scale

The first order impact would be EV service outage and shutdown of the EVCS (Acharya, Dvorkin, & Karri, 2020; Acharya, Dvorkin, Pandzic, et al., 2020; Alcaraz et al., 2023; Antoun et al., 2020; Basnet & Ali, 2021; Brighente et al., 2023; Carroll et al., 2022; ElHussini et al., 2021; Elmo et al., 2023; Garofalaki et al., 2022; Girdhar et al., 2021, 2022; Hamdare et al., 2023; Harnett et al., 2018; Johnson, Anderson, et al., 2022; Johnson, Berg, et al., 2022; Köhler et al., 2022; NESCOR, 2015; Nisar et al., 2022; Plaka et al., 2023; Reeh et al., 2019; Sarieddine et al., 2023, 2024; Skarga-Bandurova et al., 2022; Sygensys for National Grid ESO, 2022).

Studies described two second order cascading impacts:

- a) Seven studies described impacts on the transport sector: DDos attacks could result in impacts to supply-chains due to vehicles being unavailable for medical services, critical emergency services, food and agriculture, manufacturing and defence (Girdhar et al., 2021; Hamdare et al., 2023; Johnson, Anderson, et al., 2022; Johnson, Berg, et al., 2022; NESCOR, 2015; Reeh et al., 2019; Skarga-Bandurova et al., 2022).
- b) Five studies described impacts on local power distribution: The sudden drop in demand could cause degradation of power quality and local or regional blackouts (Acharya, Dvorkin, & Karri, 2020; Acharya, Dvorkin, Pandzic, et al., 2020; Basnet & Ali, 2021; Carroll et al., 2022; Sygensys for National Grid ESO, 2022). Tertiary impact - Cascading failures across multiple power grids could result in a city-wide blackout as discussed earlier.

Multiple incidents at small scale simultaneously

Two scenarios for this systemic event category were described across five studies. In the first, one study described a Denial of Service (DoS) cyber-attack with a unique second order impact wherein the attacker could take control of the user interface or charging operations and demand a ransom from users as well as the EV charging operators (Sarieddine et al., 2024). Multiple such incidents occurring simultaneously could cause severe tertiary impacts to the transport sector, although this impact was not discussed in the study.

Four studies (Jeffay, 2022; Malik & Anwar, 2022; Plaka et al., 2023; Skarga-Bandurova et al., 2022) reported an incident of cyberwarfare. In 2022, during the Russia-Ukraine war, the EV charging stations on the 450-mile highway between Moscow and St Petersburg were hacked. The EVSEs displayed supportive messages for Ukraine and charging services were denied to the users (a first order impact). Further cascading impacts were not mentioned. However, such attacks could disrupt the transport sector if most vehicles in circulation were EVs.

Multiple incidents at small scale over time

Three cyber-attack scenarios were found for this category. For the first scenario, one study described how a malicious actor could tamper with the EVSEs to harm people when charging their vehicles (Carroll et al., 2022). It could burn people's hands, and/or cause electric shock (first order impact). If incidents occurred on the same day across multiple EV charging stations in a country, they could compromise public safety, result

in a loss of trust in the EV transition and potential legal/financial/reputational impacts – second order impact (NESCOR, 2015). Tertiary impacts were not described.

In the second scenario, as reported in five studies, in May 2022 cyber criminals took control of EV charging stations on the Isle of Wight, UK (Carey, 2022; David, 2022; Malik & Anwar, 2022; Plaka et al., 2023; Skarga-Bandurova et al., 2022). The affected EV charging stations displayed pornography (first order impact). Second order and tertiary impacts were not described, however, potentially people could lose trust in EV charging stations and EV adoption.

Eleven studies described the third scenario that could lead to intentional damage to the performance of EVs and EV charging services. Hostile actors could manipulate the safety systems to intentionally overcharge/discharge the EV batteries (Brighente et al., 2023; Conti et al., 2022; Girdhar et al., 2021, 2022; Hamdare et al., 2023; Harnett et al., 2018; Johnson, Anderson, et al., 2022; Nasr et al., 2022; NESCOR, 2015; Phiri et al., 2022; Reeh et al., 2019). The first order impacts mentioned were damage to the EV battery (Conti et al., 2022; Girdhar et al., 2021, 2022; Hamdare et al., 2023; Harnett et al., 2018; Johnson, Anderson, et al., 2022; NESCOR, 2015; Phiri et al., 2022; Reeh et al., 2019; Skarga-Bandurova et al., 2022), the need to recharge the EVs often due to continuous discharge prior to the battery getting damaged and impairment to the whole charging system (Brighente et al., 2023). A second order impact could be potential damage to the performance of EVs and EVs going out of service. Tertiary impacts were not stated for this scenario.

A variation of this attack was described by Malik & Anwar (2022) who discussed how an EV charging station's power interface with EVs could be used by offenders to mine cryptocurrency. This is a computational intensive process (for a discussion, see (Khan et al., 2021; Li et al., 2019; Malik & Anwar, 2022)) that would result in the EV battery power being used quickly for the mining process and EVs needing to charge too often – a first order impact (Khan et al., 2021; Malik & Anwar, 2022). Malik & Anwar (2022) stated that there would be cascading impacts to society, climate change and sustainability (Malik & Anwar, 2022), however these impacts were not described.

Few incidents close to simultaneous succession

Four studies (Nasr et al., 2022; NESCOR, 2015; Reeh et al., 2019; Sygensys for National Grid ESO, 2022) described a cyber-attack scenario that could ignite EV batteries. A trojan horse virus could be injected into EV systems by a hostile actor, potentially through a compromised EV charging network. For the first order impact

described, the virus creates the illusion that an EV is undercharged. This would lead to a second order impact where the battery is overcharged which could eventually lead to physical safety risks such as a thermal (fire) event. This is particularly dangerous because EV fires specific to lithium-ion battery packs can reignite and special training is needed to put them out (Nedelea, 2022). It can be inferred that such incidents could have catastrophic tertiary impacts on transport services, the emergency services, as well as national security if they occur at multiple sensitive locations in a short period of time.

4.5 Discussion

The aim of the systematic literature review was to explore cyber-attacks on smart infrastructure that cause cascading impacts in connected places. The research reviewed came from, or was about, 24 different countries emphasising that the research in this field is not limited to a few geographies. Sixteen cyber-attack scenarios with unique cascading impacts (five- smart CCTV, three – smart lighting, eight – smart EV charging, zero – smart bus stops) were identified across 51 studies. Only two of these scenarios included all three types of cascading impact (first-, second- and tertiary-order impacts) but these were specific to smart EV charging. Interestingly, out of the 16 cascading scenarios identified, only five had been reported to have occurred in the real world so far – three incidents for CCTV and two for smart EV charging. However, other incidents may have occurred but not have been reported. New threats could also emerge in the future, particularly as systems are rolled out and the attack surface increases. For smart lighting systems, the US Department of Energy and American National Standard Institute (ANSI) have identified risks and provided cybersecurity strategies, standards and mitigations to protect individual components (Stellios et al., 2022a). However, the threat analysis is limited to first order cascading impacts of the connected street lighting network and specific to system architecture which may not be a helpful source for non-IT professionals to govern the resultant cyber risks. No crime scenarios that could create cascading impacts were found for smart bus stops which could be due to a lag in publication of academic literature. The above results may create a perception that the probability and impacts of cascading effects of cyber-attacks on smart infrastructure could be very low; however, connected place transformations are at an early stage and so the opportunities for crime have the potential to grow very quickly. Future work should explore using Delphi technique to

assess whether the available literature identifies sufficient cascading impacts of threats in connected places.

For smart CCTV and smart lighting, all the eight cyber-attack scenarios described were first-order cascading impacts. In contrast, large-scale cyber-attacks on connected EV charging stations aim to disrupt the services of the two CNI it connects - transport and energy. One of the prime targets for state actors and organised crime groups are the CNI, mainly the smart grid, because it can disrupt all essential services, businesses, Government functions as well as people's day-to-day activities (Kitchin & Dodge, 2019; Yilmaz & Uludag, 2021). As smart EV charging plays a big role in balancing the power grid, a cyber-attack on EV charging networks could disrupt the grid operations even if the cyber-attacker did not target the grid (Hunn, 2018; Sygensys for National Grid ESO, 2022; Zhang et al., 2019). The EV charging outages on the 450-mile highway between Moscow and St Petersburg discussed above provide a warning about how state-sponsored attacks could work in the future. The risk of lithium batteries catching fire due to multiple cyber-attacks at the same time across cities also needs to be understood better in terms of impacts on national security, emergency services, disaster recovery and fire-fighting training.

A key limitation of this study is that the insights were limited to the four specific infrastructure use cases selected. These do not represent all smart infrastructures. There could also be additional challenges from other new innovative smart infrastructure, emerging technologies, and interactions with other elements of connected places. It is possible that the risk of occurrence for some of the crime scenarios reviewed for the smart infrastructure use cases in this chapter might have changed due to recent security interventions or additional crime scenarios might have been identified since the review was completed. It is also important to note that the cascading impacts were only found for the interfacing infrastructure networks for each use case. For example, scenarios where a disruption to an EV charging service cascaded to networks other than the direct interfaces of EVSE (e.g. cascading impact to smart CCTV hosted within EV charging station) were not found. Further research is needed to understand whether this is because there are limited opportunities for such cascades to occur or because the analyses reported to date have been too limited in analysis and scope.

While the impacts discussed here cannot be generalized beyond the use cases examined, two observations apply across the case studies. First, the cascading

impacts of the five real-world incidents (three incidents for CCTV and two for smart EV charging) were potentially minimized by appropriate responses. For example, the incident of CCTV cameras being out of service in Washington DC 8 days ahead of US President's inauguration was resolved by taking systems offline and re-booting them which resolved the incident in the required timeframe without the need for a ransom to be paid (Hackread, 2017; Vennam et al., 2021). Further research is required for other cyber-attack scenarios described in section 4.4 to assess whether measures are in place to prevent the cascading impacts of cyber threats from materializing. Second, common vulnerabilities in products (such as Philips Hue LED bulbs) and infrastructure services (such as application vulnerabilities in a network of EVCS) provide opportunities to commit large scale crimes remotely across a variety of physical (not just virtual) elements with minimal effort from cyber-criminals. For example, when a local authority orders a CCTV system or EV charging services, they place large orders with the same organization. While this creates an economy of scale, it can mean that any vulnerabilities present in one camera/ EVCS application will be present in all of them at the same time, meaning that the whole system may be vulnerable. This has been referred to elsewhere as a 'class break' wherein a security vulnerability enables cyber-attacks on not just one system, but an entire class of them (Chaudhari & Zennaro, 2020). Class break resistance is about identifying the potential misuse of such common vulnerabilities and mitigating the cyber risks to prevent them being exploited (Chaudhari & Zennaro, 2020). A simple mitigation could be for local authorities to source their smart infrastructure from multiple vendors reducing the chance of common vulnerabilities. However, there is also a need to establish security mechanisms that anticipate class breaks and stay secure despite them.

There is a need for more continuous research to critically examine the potential misuse of connected street infrastructure and assess which security interventions address these challenges. Managing security risks for connected places needs to address a consistent "system of systems" approach across local, regional, city and country regimes in addition to traditional cyber security measures (such as access control and authentication) that work on individual systems (Kitchin & Dodge, 2019; Meijer, 2018). Preventative interventions such as the isolation of networks is not easy due to the need for IoT networks to stay connected to provide integrated services. Local authorities need to ensure that the threats to the connected ecosystem are understood, security measures are validated against threat scenarios and cyber risks

to a range of important services are managed (NCSC, 2021a; NCSC, 2022b). The threat landscape could change quickly due to fast-paced technological innovations and previously unknown complex linkages and dependencies evolving over time (Macaulay, 2016). The assessment of systemic risks (i.e. risk of systemic events occurring) is challenging due to uncertainties around how a failure from a cyber-attack could develop cascading impacts across multiple smart infrastructure services outside the control of organizations whose asset/infrastructure is attacked (Kaffenberger & Kopp, 2019). DSIT has recently published guidance for local authorities to develop detailed plans to conduct risk assessments for network security threat scenarios for connected places (DSIT, 2019b). Threat scenarios for connected places (not just threats from individual infrastructure, its interfaces, and networks) need to be developed based on the potential vulnerabilities of connected infrastructure operations. The Government of Ireland has published an approach to manage systemic risks that affect the CNI (National Cyber Security Centre - Government of Ireland, 2022); they have provided examples where inter-dependencies and inter-relations across connected systems are mapped to create the visibility of the systemic risks and potential cascading impacts. This approach could be customised and reused at national, regional and local levels.

As mentioned in Chapter 2, section 2.1, SCP, a criminological approach (Clarke, 1983) has shown that crime opportunities can be reduced using five different strategies – increasing effort, increasing risks, reducing rewards, reducing provocations, and removing excuses. Identifying the common vulnerabilities (for products, networks, and services) at design as well as pilot stages could reduce the attack surfaces thus increasing the effort and increasing the risks for cyber-criminals. A detailed description of threat scenarios with cascading impacts that could manifest, can help to provide a comprehensive overview of cascading risks to a connected ecosystem (Carroll et al., 2022; Kaffenberger & Kopp, 2019). It can also help city authorities and urban planners avoid building single points of failure, thus increasing the effort for cybercriminals. A focus on complete visibility of the inter-connections/digital dependencies across infrastructure services in the connected places ecosystem rather than just organizational systems, could help harden the critical interfaces and build ‘security’ by design to protect common critical assets. Organizations need to anticipate how adversaries could adapt and build systems of systems that are “fail-secure”, i.e. a failure does not compromise security functions

(National Cybersecurity center of Excellence, 2000; NCSC, 2021a, 2022b). Cyber-crime risks to smart infrastructure need to be managed through organizational, regional, and national policies as well as a regulatory regime with strong accountabilities to ensure that cyber-risks are managed by all organizations involved in the design and operations of infrastructure services within connected places (Demertzi et al., 2023). Implementing strong digital forensics and quick tactical interventions immediately after a cyber-attack by working collaboratively across public, private, academic and Government sectors can prevent copy-cat attacks (discussed in section 4.1.2), thus reducing the possibility of plausible deniability given to cyber-criminals (Baig et al., 2017).

Research suggests that the demands on local authorities for assurance, governance and accountabilities need to be accompanied by the development of capabilities required to conduct risk assessments for the cybersecurity of smart services operational in a connected place, as it requires different skills from those required from the traditional responsibilities typically carried out by local authorities (McKinlay, 2017). In the UK, the NCSC supports local authorities in the implementation of the Cyber Assessment Framework (CAF) which focuses on the required assurance process to manage the cyber risks of Network and Information systems (NCSC, 2022b). However, research is required on whether the NCSC guidance is sufficient and whether local authorities can implement the CAF to assure the security of smart integrated services operated by private operators. Although local authorities are building new capabilities, often they do not have expertise on par with the private firms leading the provision of smart solutions, and hence do not and cannot critically assess the operational security proposed by those private firms (Barns et al., 2016; Kobie, 2015). It is important to note that absent strong ownership of the smart cyber-physical infrastructure services provided at connected places, there is a national risk of security decisions being driven by the private sector which requires research to fully understand what the impacts of this might be (Barnfield, 2020; Robinson, 2023).

DSIT recommends a security approach for local authorities to break silos by conducting reviews with multiple stakeholders using best practices, governance (responsibilities and accountabilities) and relevant regulatory oversight for street infrastructure transformations (DSIT, 2022; Loia & Maione, 2022). This can be strengthened by governance platforms, improved accountabilities, timely policies and further research (Cooray et al., 2016; Milenkovic et al., 2022). Additionally, capacity

needs to be built within local authorities and procurement framework teams for specialist teams to ensure that security as well as resilience risks are anticipated beyond IT risks (Kitchin & Dodge, 2019). As discussed in Section 4.1.2 the operational security monitoring teams of private operators (acting as place managers and capable guardians) are responsible for security of their smart infrastructure. In the context of services procured by local authorities from private operators in connected places, it is important to identify, evaluate, and mitigate security risks that arise when working with the supply chain. Due diligence within the procurement programmes is essential to ensure that security is embedded by design, the cyber-resilience measures are adequate, and the supplier confirms to the required standards. The local authorities as controllers need to govern 'security by design', enforce implementation of Government's (super controller) regulations and assure the security risks of the connected place in which these services operate. The risks to be managed, if identified at a pre-contract stage can ensure the services are operated at the right level of cybersecurity through the procurement contracts by the operator. It needs to be researched whether the role of Government and local authorities as super controllers and controllers is developed within smart service procurement programmes through relevant policies and regulations (Wolbertus et al., 2020).

The ability to disrupt multiple systems including the CNI of a city remotely, needs a radical shift in how we think about resilience (i.e. minimising cascading impacts, responding to cyber-attacks, and recovering from failures) of smart cross-sector services rather than just organizational accountabilities for security. The knock on effects of cyber-crimes is a challenge for disaster recovery as well as emergency response (Kitchin & Dodge, 2019). Building appropriate and proportionate resilience to anticipate as well as recover from the impacts of cyberattacks in a connected place is crucial to the continuity of smart infrastructure services should disruption occur (Katsarov, 2023; Pratt & Carroll, 2019; Shukla et al., 2019). The mechanisms for protection against attacks on CNI require resilience strategies such as reducing risk exposure, resilience tests in anticipation of attacks, early detection of an attack to minimize the risk of cascading impacts and quick recovery. The UK Government Resilience Framework (UKGRF) has defined who leads (from UK government department, devolved administrations or other public bodies) all phases of emergency planning, response, recovery and risk assessment to strengthen crisis management processes (Gov.UK, 2022; UK Cabinet Office, 2023). However, there is a lack of

Emergency Response plans, and a mandate to conduct resilience tests for a connected cross-sector ecosystem at the required scale (Cerrudo, 2015; Kobie, 2015; Owano Nancy, 2017). Currently, efforts to develop 'resilience by design' focus more on organizational assets, interfaces, networks, and services. It is important to additionally focus on managing security risks of connected places where the cross-sector cyber, physical, and cyber-physical interactions are managed by multiple organizations. In the UK, finance, health and telecom sectors have conducted limited dry runs to test the resilience of their sectors (i.e. response and recovery in event of a cyber-incident) (Shukla et al., 2019). It is recommended that local authorities conduct similar resilience tests for cascading impacts of potential cyber-attacks in connected places where multiple smart infrastructure services operate.

The UKGRF commits to providing guidance to implement three core principles (understanding of risks, prevention strategies and 'a whole of society' approach) and six themes (risk, responsibility and accountability, partnership, community, investment and skills) (Gov.UK, 2022). The NIS2.0 directive to be implemented in 2024 (in the UK and EU) (European Commission, 2023a) and the UK's NCSC cybersecurity strategy (2022-2030) have recognised the importance of managing cyber risks to prevent and recover quickly from cascading impacts in smart urban environments (Chiara, 2022; European Commission, 2023b; NCSC, 2022c; Schmitz-Berndt & Cole, 2022; Shukla et al., 2019). The organizations implementing smart infrastructure services are required to follow best practices of assessing threats, managing vulnerabilities (including those of IoT), embedding standards and complying with regulations for the security of the people as well as in connected places (Katsarov, 2023; Yorio et al., 2018). The Department for Transport (DfT) in the UK has published a smart street manual to provide guidance for managing, operating and maintaining street infrastructure through use cases of integrated transport services (Transport Technology Forum, 2022). However, the security aspects were not specific to use cases in a way that would help city authorities create security specifications for the procurement of connected urban infrastructure services. The 'Smart street Infrastructure security' report published by the UK Government in 2022 mentions the need for additional measures for the security of smart infrastructure - risk assessment, updated Publicly Available Specifications (PAS) and operational oversight by a regulatory authority (DSIT, 2022). However, these standards, frameworks and guidelines for cyber security of connected places did not refer to any overarching

policy owned by a UK Government Department for connected places. A policy intervention and national strategy for managing systemic security risks of connected places needs to be an urgent priority. Knowledge of “what works” in terms of resolving crime issues in connected places needs to be replenished by new varieties of practical intervention methods to prevent and deter crime opportunities (Ekblom, 2017).

4.6 Conclusion

This chapter provided an overview of some of the digital capabilities and potentially criminogenic properties of a sample of smart urban infrastructure, how this might cause cascading impacts in a connected place, and the transformation of security operations. In doing so, it complements and extends the study of traditional criminogenic properties of physical urban elements in Chapter 3. The systematic literature review and its findings captured the key points for a snapshot in time, which means that any other planned future developments associated with the fast-paced technological innovations and the evolving crime landscape may not be reflected.

The IoT is gradually connecting everyone to everything, and cyber and physical security are increasingly interdependent. The risk of cascading impacts in connected places needs to be continuously assessed to determine whether it is within acceptable thresholds to ensure that the rewards of digitization in connected places are worth the investment. Sustainability agendas focus on liveability, which should automatically include safety and security elements rather than identifying the risks for the ecosystem post roll-out. More alliances need to be built to rollout smart infrastructures in an ethical way with consistent policies to assure security, resilience, and sustainability benefits.

There is potentially a lag in Government guidance, policies, benchmarks, governance, and regulations to support local authorities in managing the systemic risks, operational security, incident response and recovery from cyber-attacks within digitally connected places. Considering there have been no reports of large-scale catastrophic attacks for smart lighting columns, smart EV charging, and smart bus stops, now is the right time to analyse the potential threats, the possible efficacy of security interventions and preparedness for recovery from hostile incidents. Further research is recommended to develop cyber-attack scenarios with potential cascading

impacts that can help urban planners and local authorities (place managers) create a secure environment.

The UK Government now supports local authorities to shift their focus from the cyber-risk management of services they procure from individual organizations to additionally think about the impacts of cyber-attacks in the whole connected place ecosystem. However, there is limited research on security and the implementation of 'resilience by design' and management of systemic risks for projects managed by local authorities. It is important to understand this and how the risks of cascading impacts in connected places are managed. Since such projects are at an early stage of maturity, a more detailed study in this area would help to establish security best practices, policy interventions by the UK Government and challenges faced. This is the aim of Chapter 5.

Chapter Five

5 Assessment of current security measures in connected places

As seen in the prior chapter, the cyber-attacks on smart infrastructure services such as EV charging can cause cascading impacts to the Critical National Infrastructure (CNI) services. The need for cross-sector operational service resilience, meaning the quick recovery from a security incident with minimal damage, has long been recognized by the Government, public and private organizations as being one of the most critical pillars of the connected street infrastructure (NCSC, 2022b; Greater London Authority, 2020). Reacting quickly to an incident, as soon as the first evidence of a cyber breach is detected, is becoming more important than ever because cyberattacks can quickly spread across the country and beyond when the infrastructure services are connected within smart cities (Blythe & Johnson, 2021; NCSC, 2022b). There is a real risk of a hostile country gaining access to insights into the day-to-day activities of people across sensitive locations and organising cyber, physical or cyber-physical attacks (Chaudhuri & Bozkus, 2023; Demertzi et al., 2023; Lessambo, 2023; Papaiakevou et al., 2022; Vanberghen, 2022). Local, regional and national authorities need to ensure that the threats of systemic events in the connected ecosystem are understood, cyber risks to a range of important services are managed, prevention measures are built in by design to mitigate the cascading impacts and the operational cyber risks of smart services are governed (NCSC, 2021a; NCSC, 2022b).

The Local Authorities (LAs) engage private operators for the installation and operations of smart services in connected places. LAs' commissioning process involves (i) defining specifications for smart service installation as well as operations, (ii) inviting suppliers to submit bids (also known as tendering), (iii) evaluating the supplier offerings, (iv) selecting a supplier offering, (v) signing a procurement contract with the selected supplier, (vi) managing, as well as assuring, the contract deliverables, and (vii) assessing, as well as refining, the procurement process (LGA, 2019). The purpose of this study is to explore whether the current procurement process for smart infrastructure services enables the LAs to minimize cyber-resilience risks to the CNI services in the connected places.

5.1 Aim, Research questions, and approach

The National Cyber Security Centre (NCSC)'s cybersecurity principles for connected places aim to help authorities understand the security risk mitigation measures required to ensure that connected places, as well the underlying smart infrastructure are designed, built, and operated in a secure as well as resilient manner; and the systemic risks are managed (NCSC, 2021b). The NCSC guidance is intended for risk owners, designers and personnel involved in the day-to-day operations of smart infrastructure, as well as smart service functions within connected places (NCSC, 2021b). The approach taken in this study was to use the NCSC cybersecurity principles for connected places as a baseline for reviewing the security and resilience specifications in the procurement contracts used for smart services. The aim of this study was to explore whether the NCSC cybersecurity principles for connected places were embedded in the smart service procurement processes by the LAs and whether that supported the LAs in governing the cyber-resilience risks to the essential Critical National Infrastructure (CNI) services in connected places.

The research questions were a) Do the procurement contracts for smart services specify measures for cyber security and resilience in line with the NCSC cybersecurity principles for connected places? and, b) Are there any challenges in managing the cyber resilience of the connected places (while implementing the governance and assurance mechanisms as provisioned in the procurement contracts)? Due to the nature of IoT technologies used in smart infrastructure, the lines between physical and digital infrastructure are becoming blurred (Vermesan et al., 2020). Consequently, the physical and cyber-physical risks to the operational security of connected places are also considered within the scope of this study.

The study focuses on procurement requirements agreed by the LAs with the operators of smart services and hence excludes the internal agreements made by the operator with their supply chain. Technical architecture and technical design details for the Network and Information Systems (NIS) and IT administration (such as data loss, identity theft, authentication, and access) are within the scope of the smart service operator's detailed designs and compliance requirements within the procurement frameworks. Hence, the scope excludes an exploration of the detailed architecture, technical designs, and IT administration aspects of the service providers which is internal to the operator's offerings and not governed by LAs. However, the

governance of supply-chain risks and assurance of service provisions are within the procurement process managed by the LAs and are included in the scope of work.

5.2 Study Design

The study in this chapter (see Figure 5-1) involved three stages: 1) Stakeholder identification and preparation, 2) Data gathering and, 3) Further analysis. A high-level overview of these stages is described below, while further details are provided in the sections that follow.

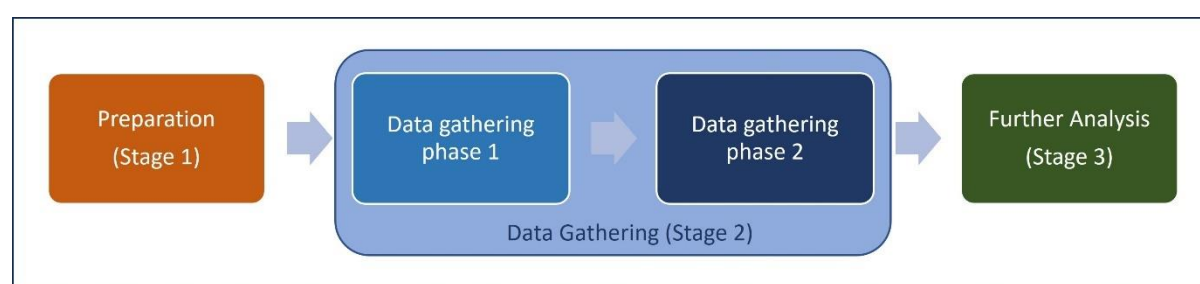


Figure 5-1 Overview of Study Design

5.2.1 Methodology

The preparation (stage 1) involved sampling of the NCSC cybersecurity principles for connected places, selection of a use case for this study and identification of stakeholders to be invited to participate in the study.

Data gathering (stage 2) was completed in two phases. In phase 1, the stakeholders were introduced to the aims of the study, basic data was gathered through interviews and the selected use case was validated to ensure there was sufficient data available for analysis of the procurement process. Expert stakeholders were identified to form a focus group and engaged for regular discussions with the researcher to help elicit their knowledge on application of the NCSC connected place guidelines for cybersecurity. Focus group methodology has been used by researchers wherein regular meetings are facilitated by the researcher to promote discussions with experts, share ideas as well as gather multiple perspectives and insights into the data gathered (Hunt & Young, 2021; Wilkinson, 1998). In phase 2, a questionnaire was prepared to guide semi-structured interviews with the stakeholders. Semi-structured interviews were conducted with professionals in the field of smart street infrastructure design, connected place security and the procurement of smart services. Several

approaches to data collection, such as the use of structured interviews, could have been adopted but semi-structured interviews were chosen (Piroozfar et al., 2019; Clancey et al., 2014; Evans & Kebbell, 2012) as they would allow for the discovery of information that was important to the stakeholders (who are experts in their field) but that may not have been previously identified by the researcher (and hence might not be elicited using a structured survey).

During Further Analysis (stage 3), issues were identified and analysed using a thematic analysis, a qualitative analysis method used to identify key patterns/ themes in qualitative data (Ayres, 2007; Thomas & Harden, 2008). Root cause analysis (Oliveira et al., 2022; Ursprung & Gray, 2010), which is a methodology used to identify the root of a problem rather than its symptoms, was conducted for each theme using a technique termed the ‘five whys’ (Card, 2017; Ursprung & Gray, 2010). ‘Five whys’ is an iterative interrogative technique wherein up to five iterations of asking “Why did this happen?” explores the cause-and-effect, with the aim of identifying the underlying root cause of the problem (Card, 2017; Ursprung & Gray, 2010).

The UCL Department of Security and Crime Science’s ethics committee reviewed the research plan for this study and provided ethical exemption as the overall risk to the researcher and the stakeholders who participated was assessed to be very low.

5.2.2 Stage 1-Preparation

The steps for the first stage of the study are described in Figure 5-2. Criteria were developed to select security measures from the NCSC cybersecurity principles for

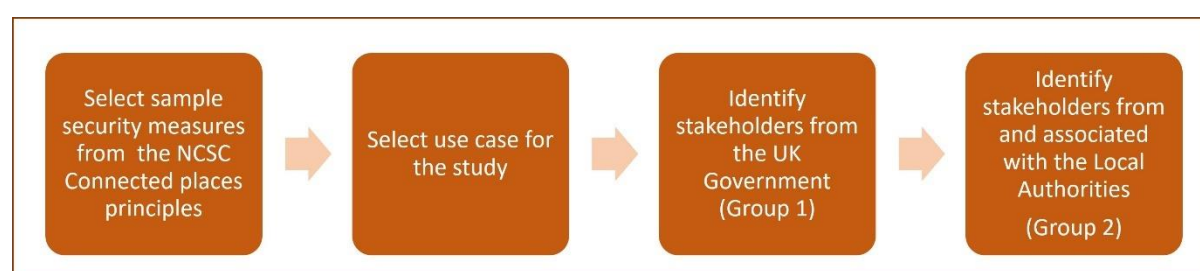


Figure 5-2 Stage-1 of the study – Preparation

connected places (see below) and for identifying the stakeholders. Given the scope of the study, at this stage, two groups of stakeholders were identified and invited to participate. Group 1 included stakeholders from the UK Government in charge of

designing and implementing policies for connected places. Group 2 included stakeholders associated with LAs who oversaw defining and implementing the connected place security guidelines and policies.

5.2.2.1 Sampling for the security measures

The focus of this assessment was to understand whether the LAs have used the NCSC cybersecurity principles for connected places to create specifications, and whether they assure as well as govern cyber risks within their procurement, operations, and contract management. The scope of the study was to assess measures in the procurement processes of smart services, that enable mitigations for managing, assuring, and governing cyber risks to the connected place ecosystem. Hence, the following inclusion criteria were developed to select the NCSC cybersecurity principles for connected places that map to the scope of this study – the principles should:

- a) Identify dependencies within the connected place ecosystem and maintain security levels of the ecosystem proportionate to the cyber risks originating from these dependencies.
- b) Point to considerations for the adequate management of resilience by design and response as well as the recovery of smart services in the event of a cyber-attack.
- c) Relate to processes that assure and govern the supplier's management of operational cyber risks.
- d) Be about processes to ensure that there is accountability for cyber risks within the connected place.

Based on the exclusion criteria discussed in Section 5.1, the following principles were excluded from this study, those that provided measures regarding:

- i) Technical architecture and technical design details for IT systems
- ii) Data loss, identity theft, authentication, privileges, and access

The fourteen NCSC cybersecurity principles for connected places were reviewed to understand whether they met the above inclusion criteria. Table 5.1 shows the NCSC cybersecurity principles that were included/excluded on this basis.

Table 5.1 Selection of NCSC cybersecurity principles for connected places

NCSC cybersecurity principles for connected places	Meets inclusion criteria				Meets exclusion criteria	
	A	B	C	D	E	F
#1 Understanding your connected place and the potential impacts	v					
#2 Understanding the risks to your connected place		v				
#3 Understanding cyber security governance and skills				v		
#4 Understanding your suppliers' role within your connected place		v	v			
#5 Understanding legal and regulatory requirements	v			v		
#6 Designing your connected place architecture					v	
#7 Designing your connected place to reduce exposure (detailed design aspects)						v
#8 Designing your connected place to protect its data (aspects of data architecture and design)						v
#9 Designing your connected place to be resilient and scalable		v	v			
#10 Designing your connected place monitoring	v	v	v			
#11 Managing your connected place's privileges						v
#12 Managing your connected place's supply chain		v	v			
#13 Managing your connected place throughout its life cycle	v			v		
#14 Managing incidents and planning your response and recovery		v	v			

5.2.2.2 Selection of a use case

The four use cases (smart CCTV, smart lamp posts, smart EV charging and smart bus stop environments) discussed in the literature review (see Chapter 4, section 4.2.1) were assessed as to their suitability for detailed investigation and data gathering. It was important to analyze the governance and risk mitigation strategies within the procurement contracts of the LAs, that assure that any cyber-attacks on smart infrastructure services are contained rather than cascade quickly to the CNI within the connected place ecosystem. Cyber risk exposure depends on the level of “smartness” of the services implemented in each LA, i.e., the amount of integration of smart services with other essential services in the ecosystem. Hence the use cases were assessed against the following criteria:

- A) There must be a proven existing example that a cyber-attack on the smart infrastructure considered has disrupted/ affected CNI services through cascading impacts of second and third order (see Chapter 4, section 4.3 for explanation of cascading impacts).
- B) The extent to which the infrastructure for the smart public service was connected / planned to be connected digitally to CNI to provide public integrated services.

The cybercrime scenarios outlined in the literature review (see Chapter 4, section 4.4) provide recent examples of the disruption to transport services and energy services through a cyber-attack on smart EV charging service. The second and third order cascading impacts of cyber-attacks to the CNI sectors were found only for the EV charging use case. In the UK, the EV charging infrastructure was extensively connected to two essential CNI– transport and energy to provide integrated services to the public (EV Energy Taskforce Working Group 3, 2021). The UK aims to lead on the transition from gasoline/diesel vehicles to EVs and EV charging stations (EVCS) (Energy Systems Catapult, 2020; HM Government, 2022). Hence, the EV charging use case was the only one that met both the selection criteria and was included in the scope of this study. Criteria B also required the smart services to be available to the public. Hence, only the public EV charging services on streets were considered; residential and commercial/ office charge points within private premises were excluded. The selection of use case was validated with the stakeholders in the LAs (discussed in Section 5.3.1.3) to ensure that sufficient data is available from the procurement processes of EV charging services.

5.2.2.3 Identification of stakeholders from the UK Government (Group 1)

Table 5.2. summarises the stakeholders identified from UK Government departments. The rationales for including these stakeholders are as follows. As noted in the literature review, ‘The Manual for streets’ is used in the UK for the design, construction, adoption, and maintenance of new streets as well as existing residential streets subject to re-design. As ‘The Manual for streets’ is the primary responsibility of The Department of Transport (DfT) in the UK, the head of street design policy in charge of the Manual for Streets at DfT was selected as the first stakeholder. Snowball sampling was used to identify the remaining relevant stakeholders associated with smart streets for participation in the study. The DfT stakeholder mentioned that they had commissioned the Connected Places Catapult to develop a Manual for Smart streets that focussed on designing digital urban infrastructure services within the connected places (Transport Technology Forum, 2022). Hence, two stakeholders working on the Manual for smart streets (for two different use cases) at the Connected Places Catapult were selected as participants. The DfT stakeholder working with them was also included as a participant for this study. The DfT also provided references to the Centre for protection of National Infrastructure (CPNI) (now known as National

Protective Security Authority (NPSA)) dealing with the security standards for connected places, who agreed to participate in the study.

Table 5.2 Stakeholders identified from the UK Government (Group 1)

Organization	Number of Stakeholders	Stakeholder References	Description
Department for Transport (DfT)	2	DfT-SH1, DfTSH2	DfT stakeholders in charge of updating the street design manual and commissioning of the Manual for smart streets
NCSC Connected Places Team	2	NCSC-SH1, NCSC-SH2	National cyber security centre (NCSC) stakeholders in charge of designing and supporting the cybersecurity principles for connected places
Centre for protection of National Infrastructure (CPNI)	1	CPNI-SH	Centre for Protection of National Infrastructure (CPNI) stakeholder in charge of guidelines for personnel and location security for connected places
Senior policy advisor, UK Government	1	PA-SH	Stakeholder from the team developing the policies for secure connected places
Department for Science, Innovation, and Technology (DSIT)	1	DSIT-SH	Stakeholder from the team supporting the policies for secure connected places.
Connected Places Catapult	2	CPC-SH1, CPC-SH2	Additional stakeholder working with the department in charge of smart street design policies commissioned by the DfT

As the purpose of the study was to analyse the implementation of NCSC cybersecurity principles for connected places, the NCSC team that published the guidelines for the security and resilience of connected places was approached through on-line contact information. Two stakeholders from this team agreed to participate in this study. The NCSC Connected places team sent a recommendation to policy advisors in UK Government to support this study. Ultimately, a senior stakeholder from the “Connected places” policy team agreed to take part. The policy advisor mentioned that The Department for Science, Innovation, and Technology (DSIT) (formerly The Department of Digital Culture Media & Sports – DCMS) manager had been supporting an Alpha Testing project since 30 Sep 2022 (which is independent from this research), established at a national level, to understand how to support the local authorities to implement the NCSC principles (Plexal, n.d.). Hence, the DSIT manager was approached, who then agreed to take part in the study.

Table 5.2 includes stakeholder “references” that enable the organisations to which they belong to be identified, without naming the individuals themselves. The research data, analysis and outputs could be sensitive and hence, were shared for

future publications only based on approvals from the stakeholders. Quotes were attributed to the individuals per organization unless they requested that they be kept anonymous.

5.2.2.4 Identification of Group 2 stakeholders from the Local Authorities

This study required the participation of highly skilled professionals from the LAs (and organizations associated with LAs) (Group 2) who were experts in collating procurement specifications for smart infrastructure, assess secure service operations, manage cyber risks for smart services, test cyber resilience needs, conduct security audits, and govern the connected infrastructure within the smart connected place ecosystem. Being the capital of the UK, London has many attractive targets for terrorists including the Houses of Parliament, resulting in high demands for security. As such, London is one of the important smart cities, not just in the UK but also across the world, where trials involving advanced technologies are encouraged (Blackwell, 2022; Department for Business, 2018; IESE Insight, 2022; Say, 2023). Based on Info security magazine, London was also subject to the highest rate of cyber-attacks in the UK, having as many as one million cyber-attacks per month (Hill, 2022; Muncaster, 2019). Hence it was felt important to ensure that at least two of the sampled the LAs were in London. Including two LAs from London enabled the researcher to also check for consistency of measures within London compared to other cities in the UK. Additionally, it was decided that at least two LAs should be sampled from other geographies within the UK to enable comparisons with each other as well as LAs within London. Hence the sample size was limited to 4 professionals from different LAs in the UK. The criteria used to identify the stakeholders within the LAs were as follows:

- A) At least two stakeholders had to be from the LAs in London and two from other LAs in the UK (see above)
- B) The stakeholders must have at least 5 years of experience of working in the LAs and must have full knowledge of procurement processes: Five years was deemed a reasonable period for the stakeholders to be aware of the full procurement lifecycle for smart services and to understand how specifications in the procurement contracts enable the management of cyber risks.
- C) The stakeholders had to have been involved in the procurement of smart public services, preferably for the selected EV charging use case.

- D) The stakeholders must agree to commit at least 2-3 hours of their time to participate in this study: It was estimated that understanding the requirements of the study, providing data by consulting with their team (due to the nature of the topics), validating the data capture and reviewing the findings from the study would need at least 2-3 hours of time from the study participant.

The London Office of Technology and Innovation (LOTI), and Local Government Association that support the UK LAs were approached to identify the stakeholders within the LAs associated with the procurement of services for smart EV charging use case. LOTI and the LGA were informed of the aims of the study and the criteria to be used to identify stakeholder participants. They identified stakeholders from four LAs across the UK who they felt would meet the study criteria, these being The Royal Borough of Greenwich, Westminster, Kingston & Sutton, and Milton Keynes. Based on further recommendations from the stakeholder participants identified so far, the head of procurement services in Manchester city local authority, Transport systems project manager from York, and the programme manager for smart services at Coventry, were contacted and they agreed to participate in this research. Ultimately, seven stakeholders agreed to participate, of which three were London-based. This met the requirements for the sample size to be four or more (see above), and for at least two of the LAs to be based in London. The researcher was further advised by the LGA that Transport for London (TfL) owned the rollout of procurement frameworks for EV charging and services for smart bus stops to support the LAs. Hence, a TfL stakeholder was approached and added as a research participant.

Table 5.3 summarises the identified stakeholders associated with the LAs (Group 2). The lead stakeholder from each organization introduced any (additional) relevant stakeholder that needed to be included in the discussion for specific topics. However, the responsibility for the content provided was with the lead stakeholder. The stakeholders were assigned references LA-1 to LA-8 (see Table 5.3). Seven out of eight stakeholders had either worked on the procurement (or procurement framework) for EV charging operations, or the upgrading of standalone EV charging services to smart services in their LAs. One stakeholder had been involved in a procurement framework for EV charging. All the stakeholders had procured at least one of the three smart infrastructure services (smart lamp posts, smart EV charging stations and smart bus stops) for their LAs. They also met criteria B-D specified above.

Table 5.3 Stakeholders associated with the UK's LAs (Group 2)

Organization	Number of lead Stakeholders	Stakeholder reference
Westminster local authority	1	LA-1
Kingston and Sutton local authority	1	LA-2
York local authority	1	LA-3
Milton Keynes local authority	1	LA-4
Manchester local authority	1	LA-5
Coventry local authority	1	LA-6
Transport for London (TfL)	1	LA-7
The Royal Borough of Greenwich local authority	1	LA-8

5.2.3 Stage 2-Data gathering

The data for this study was gathered in two phases (see Figure 5-3). In the first phase, initial interviews were held with all stakeholders in Group 1 (UK Government stakeholders) and Group 2 (LA and associated stakeholders) to understand i) the smart street security guidelines and policies at national level, and ii) the procurement process followed by the LAs for the EV charging use case. The second phase of data gathering was conducted by interviewing the stakeholders from Group 2 who had already participated in the initial phase of data gathering. A detailed questionnaire was prepared for the second phase to understand the security and resilience risk mitigation measures applied in the procurement specifications and whether they conformed to the NCSC Connected places cybersecurity principles. At this stage a focus group (Group 3) was formed (explained further in iii below). Meetings were arranged by the researcher with the focus group (Group 3) to get expert insights into the data collected and later, to brainstorm the impact of the observations from Further Analysis (stage - 3). The steps in the first and second stages of data gathering (see Figure 5-3) are illustrated below.

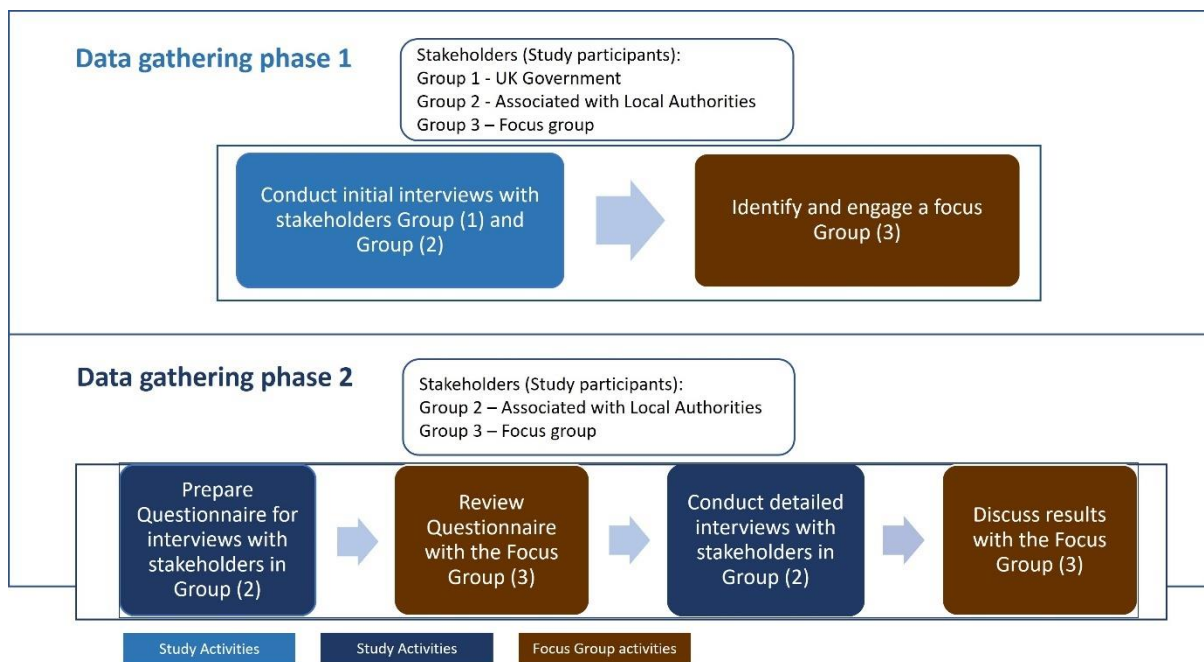


Figure 5-3 Stage-2 of the study – Data Gathering

5.2.3.1 Data Gathering – Phase 1

i) Interviews in the first phase of data gathering

Interviews were conducted March–December 2022 individually with all stakeholders and lasted about one hour. The purpose of these initial interviews was to a) introduce stakeholders to the aims of the research and understand their role in building connected places in the UK; and b) gather data on how their work contributes to the security of connected places and validate the selected use case. Three high level open questions were asked:

Q-1 Can you provide an overview of the smart street security guidelines and policies that you use in your role?

Q-2 Can you explain the cyber risk management process within the procurement process for smart services?

Q-3 Do you know whether the LAs in the UK have rolled out smart infrastructure based public services specific to four initial use cases for this study (CCTV, lamp posts, EV charging and bus stops)?

Notes from the interviews were taken by the researcher and shared with the stakeholders as minutes of the meeting to ensure accuracy. The use cases were reviewed by stakeholders. According to the eight stakeholders associated with LAs,

the smart CCTV, smart lamp posts, as well as smart bus stop environments, did not materially provide any integrated digital services with the CNI in the areas governed by their LAs. Six of the eight stakeholders pointed out that the smart lamp post rollouts in the UK were mainly focussed on energy saving measures and only a few sensors were installed on lamp posts (examples provided included Movement sensors/retrofitted cameras that detect objects and transmit data to count vehicles as well as pedestrians). As a result, any cyber-attack on a lamp post network might only impact the streetlight availability in a small area. A similar view was collectively expressed for bus stops. Five out of eight stakeholders mentioned that the primary focus of smart bus stops in the UK is to earn revenue through digital adverts, provide CCTV for security, and to display the arrival times of buses in real-time. As LA4 put it, a cyber-attack on the smart features of bus stops would only result in “*potential disruptions to the bus stop schedule display or other digital advertisements at the bus stop*”. Such information may be available through other sources such as mobile apps and is not critical to the essential service. Stakeholders also agreed that the CCTV is not expected to be directly used to commit crimes to disrupt essential services in the connected place ecosystem (Piza et al., 2019a, 2019b), but is expected to be used to prevent them. All eight stakeholders (see Table 5.4) confirmed that smart EV charging was appropriate use case for this study.

LA stakeholders advised that a smart EV charging operator should be included in this study to gain more perspective on the associated operational cyber security and resilience risks. As a result, ten private EV Charging Point Operators (CPO) were contacted through the contacts provided by the LAs and further snowball sampling. Residential and commercial/ office charge points are within private premises and not on streets and hence the operators of these charge points were not approached. Two of the five stakeholders that responded to the request to participate met the study inclusion criteria; however, only one senior stakeholder out of the two was willing to participate and was included in the study. This stakeholder is referenced as CPO-1 (see Table 5.4).

At this stage, further interview requests were sent to all the stakeholders. LA8 a stakeholder from Group 2 (see Table 5.3) reported that that the Greenwich borough had a limited number of EV charging stations, that they were not aware of NCSC cybersecurity principles for connected places, that they were working on Greenwich's revised EV strategy and hence were unable to share any further information.

Consequently, a total of eight stakeholders (see Table 5.4) took part in the more detailed semi-structured interviews.

Table 5.4 Stakeholders in Data gathering Phase 2 to study procurement of smart services

Organization	Number of lead Stakeholders	Stakeholder reference
Westminster local authority	1	LA-1
Kingston and Sutton local authority	1	LA-2
York local authority	1	LA-3
Manchester local authority	1	LA-4
Milton Keynes local authority	1	LA-5
Coventry local authority	1	LA-6
Transport for London (TfL)	1	LA-7
EV charge point operator (Anonymous)	1	CPO-1

ii) Identify and engage focus group stakeholders

As mentioned earlier, as Connected places is a very specialised field, a focus group (Group 3) led by the UCL researcher was employed to tap into the knowledge of the experts to validate the observations made during data gathering and the inferences drawn during the analysis phase. The connected places team within the NCSC are the technical authority on the security of smart services and own the principles of Security for Connected places. Consequently, they were invited to (and did) join the focus group. This team further recommended and facilitated the inclusion of the stakeholders in charge of designing and supporting the security of smart EV charging services. Senior policy professionals from the UK Government teams facilitate the creation of security policies for smart streets and assess the implementation challenges faced by the LAs. Hence, one senior policy professional from UK Government was also requested to be a part of this focus group (see Table 5.5).

Table 5.5 Stakeholders identified for the focus group (Group 3)

Organization	Number of Stakeholders	Stakeholder References	Description
NCSC Connected Places Team	2	NCSC-SH1, NCSC-SH2	National cyber security centre (NCSC) stakeholders in charge of designing and supporting the cybersecurity principles for connected places
Senior policy advisor, UK Government	1	PA-SH	Stakeholder from the team developing the policies for secure connected places
NSC Energy Team	1	NCSC-SH3	National cyber security centre (NCSC) stakeholders in charge of designing and supporting the security of smart EV charging services
UCL Researcher			Facilitate focus group meetings

The objectives of the focus group were as follows:

- i) To ensure that the questionnaire for the Group 2 stakeholders mapped onto the NCSC cybersecurity principles for connected places.
- ii) To seek clarifications for any questions raised on cybersecurity requirements for smart EV charging services procured by the Group 2 stakeholders, and
- iii) To gain an in-depth understanding of the impact of the analysed data on the NCSC guidance and policies for connected places (stage 3)

Six focus group meetings were held (every two weeks for three months) after the data gathering stage began. The researcher provided the objective, and outputs from the data gathered and/or analysed by email in advance of the (online) meetings. During the meetings, the researcher took the role of the moderator to explore the group's perspective of the interpretations of the data gathered, understand the impacts of the analysed issues, feasibility of suggested resolutions, gaps in NCSC guidance and to validate the researcher's ideas on recommendations. The minutes of the meetings were captured and shared with the focus group members.

5.2.3.2 Data gathering – Phase 2

The second phase of data gathering consisted of preparing the questionnaire and conducting interviews with the stakeholders.

i) Preparation of Questionnaire

A questionnaire, shown in Table 5.6, was created using the NCSC cybersecurity principles for connected places. This was sent to the focus group who were asked to validate the questions and to ensure that they were in line with the principles. The group requested no changes, and the questionnaire was used for the semi-structured interviews.

Table 5.6 Research Participants and Questionnaire for second phase of data gathering

A. General Questions formulated by the researcher
1) How are the responsibilities shared between the LA and the operator for smart service rollouts? 2) What is the process of including security and resilience requirements in the procurement contract? 3) Are you aware of the potential cyber-crime scenarios for the smart services procured? 4) Are you aware of NCSC's Connected places guidelines? (https://www.ncsc.gov.uk/files/NCSC-Connected-Places-security-principles-May-2021.pdf). 5) When you procure smart infrastructure services, do you use these principles to identify, as well as manage, the security and resilience risks of connected places?
B. Questions extracted from the guidance with the NCSC cybersecurity principles for connected places
#1 Understanding your connected place and the potential impacts: <i>The first step is to gain a clear and complete understanding of your connected place goals and ambitions. Who has overall responsibility and accountability for your connected place? What external dependencies does your connected place have on other systems within the street eco system? What is externally dependent on your connected place?</i>
#2 Understanding the risks to your connected place: <i>You need to have a clear understanding of your connected place infrastructure by identifying, understanding, and assessing inter-dependencies. Have you understood the resilience needs, vulnerabilities and threats to connected places? Have you identified risks that you can prioritise according to how concerning they are and what impacts are unacceptable?</i>
#3 Understanding cyber security governance and skills: <i>Your connected place cyber security needs to be owned, governed, and promoted at the top level of the organisation. This accountability cannot be outsourced to suppliers. Do you own and govern the risk structure for both service resilience and user privacy? Do you have the right security, business, and technical knowledge to enable them to make effective and timely risk management decisions? Does the connected place have the resources and funding available for its upkeep such as operational security and improving future services and building new capabilities in line with technological advances?</i>
#4 Understanding your suppliers' role within your connected place. <i>You cannot outsource your accountability to your suppliers, as you are the overall risk owner for your connected place. Do you consider your suppliers' roles as part of your overall risk management governance process in building and operating your connected place? What assurance requirements are built into your connected place supply chain, and how these are going to be reported to you and your suppliers? For example, what is the plan to deal with the risks to connected place ecosystem and its services due to a supplier taken over by a foreign corporate group? How your suppliers will report any suspicious or malicious activity and assist you when needed.</i>
#5 Understanding legal and regulatory requirements. <i>Do you ensure that the data architecture of your connected place infrastructure is built and configured to fulfil the regulatory requirements set out in the GDPR and the Data Protection Act 2018? Do you also consider any future legal and regulatory requirements that may currently influence your connected place?</i>
#9 Design your connected place to be resilient and scalable <i>Planning needs to be part of your connected place's design, to allow for your systems to be easily scaled, and resilient to attack. Do you define acceptable levels of service, requirements for resilience to attacks and the speed at which the system should scale to meet any increased demand?</i>

#10 Designing your connected place monitoring: Your monitoring design should give you visibility of all aspects of your connected place system, including endpoints and network edge devices. Is the connected place monitoring system independent from the operational connected place systems? Is the baseline view of the normal cross-service operations across supply-chain of connected place created and monitored to identify anomalies and report as well as assist in resolving suspicious activities. Is your supplier actively monitoring and reporting the threat landscape and adjusting the protections that they have in place to deal with these threats?
#12 Managing your connected place's supply chain Supply chain controls need to instil confidence and trust to ensure your connected place has the right levels of protection. Have you established a minimum set of cyber security and functionality expectations and hold your suppliers to account contractually throughout the whole system life cycle? Has the LA and the operator performed risk assessments to understand the supply-chain risks? Do you have the mechanisms (or criteria) to check that the protections your supplier has in place meet the level of security required for your connected place? Do you implement the 'right to audit' into all contracts and exercise this?
#13 Managing your connected place throughout its life cycle: Your supplier supports your connected place throughout its lifetime. How readily you can change suppliers, should the need arise, and the level of support required to do so? How do you test your systems throughout their lifecycle to assure required security levels?
#14 Managing incidents and planning your response and recovery: Connected places should be demonstrably resilient. How is the following handled across various operators and supply-chains? a) Building a cyber security incident response team (CSIRT) b) Acceptable levels of service c) Incident management, response plan and recovery of services d) Accountabilities and liabilities Note: Is there any dry run or walk through of recovery process in place based on lessons learnt or otherwise?

ii) Detailed interviews with the stakeholders

Interviews were conducted (and lasted approximately one hour) with each stakeholder associated with LAs (Group 2) between April 2022 and Jan 2023. The EV charging procurement specifications from the contracts already issued by the stakeholders were discussed. The researcher asked all the questions from the questionnaire (see Table 5.6), while ensuring that the interview did not restrict the information that the stakeholders could provide, including topics that may not have been covered by the questionnaire. Potential crime scenarios specific to EV charging identified in the literature review (see Chapter 4, section 4.3.4) were discussed with the stakeholders. Stakeholders were also asked to elaborate on the key challenges and issues faced in identifying the crime risks and applying the security measures using NCSC guidelines. The answers provided were documented and shared with each individual stakeholder for verification. Documents and links were also provided by stakeholders to support the information provided by them during the interviews. Permissions were sought and provided by the stakeholders to include their input in the material collected. The

researcher progressed with the interviews and began noting emerging themes. The patterns observed in the interview notes were discussed with the focus group members. The security and resilience measures reported by the stakeholders were assessed against the guidance specified in the NCSC Connected Places guidelines.

5.2.4 Stage 3- Further analysis

In the third stage of the study, data were further analysed as per the steps shown in Figure 5-4.



Figure 5-4 Stage-3 of the study – Further Analysis

The guidance within the NCSC cybersecurity principles for connected places were reviewed against gaps in the procurement processes and discussed with focus group members. Since multiple non-conformances were observed across the data gathered, a thematic analysis (see section 5.2.1) was conducted to understand the key themes including gaps, barriers, and challenges. The gaps were organised under five themes. Root cause analysis using a technique termed the ‘five whys’, a methodology used to identify the root of a problem rather than its symptoms (see section 5.2.1), was conducted for each theme and solutions recommended. The analysis, observations and findings were discussed with the focus group. The findings from this study were shared with all study participants.

5.3 Results from Stage 2 (Data Gathering)

The sections below provide the results from data gathering phases 1 and 2. Data gathering phase 1 results are the collated responses from the initial interviews (see section 5.2.3) which were held with all stakeholders in Group 1 (UK Government stakeholders) and Group 2 (stakeholders associated with LAs). Data gathering phase 2 results were specific to a) the general questions posed to Group 2 regarding the

security practices followed for the procurement of smart services and, b) the questions specific to how NCSC cybersecurity principles for connected places are implemented in the procurement processes for smart services. The observations from the results were then analysed for gaps and discussed. There is a limitation that needs to be recognised upfront, the results and observations are specific to the sample of study participants and hence these may not be generalisable. However, the results provide powerful insights into potential challenges.

5.3.1 Results – Stage2 - Phase1

The responses from the stakeholders were organised to understand three areas a) the changes to street design policies and standards defined by the ‘Manual for Streets’ considering the smart elements within the streets, b) guidance provided by the NCSC cybersecurity principles for connected places and c) the procurement process followed by the LAs for smart services.

5.3.1.1 Street design policy and standards

The DfT stakeholder mentioned that the street design policies defined by the ‘Manual for Streets’ were being updated by incorporating the new elements of the streetscape and associated frameworks. However, it did not address practices to counter security impacts of the digitally connected smart street elements. The primary focus of the street design policy, as mentioned by DFT-SH1 was *“to provide a set of basic principles and to update the existing manual with additional street elements (such as digital kiosks, e-scooter) as well as the changed frameworks”* (such as planning of street space for walkability/cycling, better inclusivity, improved accessibility, and use of e-mobility). DFT-SH1 also explained that the Manual for smart streets, which is another initiative from DfT is separate to the Manual for streets; it addresses the LA’s needs to map the smart service procurement process to standards and provide operational standards using case studies. However, it is a work-in-progress, to be rolled out in 2023 and is yet to include cyber resilience risk measures to the required level of detail. This work was commissioned by the DfT to the Connected Places Catapult (CPC) through the Transport Technology Forum (TTF). A separate initiative had been launched to create a Manual for smart street services to support the LAs with the procurement and governance of smart street services.

As per the information provided by CPC-SH1, *“CPC were developing and publishing a set of 12 ‘Smart Streets Use Cases’ that outline a high-level illustration of the functions, or a user journey being delivered as a smart service through interlinked systems and connected infrastructure”*. The purpose is to help users and the LAs conceptualise how the entire service lifecycle maps to the standards (from conception, through procurement, its operational life and decommissioning), so that a meaningful business case can be developed upon further investigation as well as detailed design. The EV charging use case was one of the 12 use cases in the beta version of the Manual for smart streets, for which a link was provided (Transport Technology Forum, 2022). It provided the detailed guidance and the mapping of standards for information and management services that support the accessibility and operations of the smart infrastructure services. The researcher reviewed the unpublished document with CPC-SH2 and noticed that the guidance also covered detailed legal and regulatory requirements for safety, as well as information security. CPC-SH2 stated that *“cyber-crime risk analysis as well as security mitigations should be the next step in the information that they need to generate.”* Six months after the discussion, the researcher was informed by DfT- SH2 that a cyber risk section is being created with the support of DfT for the Manual for smart streets. This was then discussed with DfT-SH2 who noted that generic cyber security guidelines will be included in the Manual for smart streets which was due to be rolled out in the first half of 2023. Additionally, CPNI-SH explained that *“the BSI’s PAS 185:2017 commissioned by NPSA provided specifications for applying holistic measures that are appropriate and proportionate to the risks.”*

5.3.1.2 Guidance for cyber security of Connected Places

During the initial interview, NCSC-SH1 from the NCSC Connected places team, pointed out that they had published the Secure Connected Places Guidance Collection (DCMS, 2021) to ensure that all the guidance provided by the Government for security decisions towards connected place design and operations would be available in a comprehensive format. Although BSI’s PAS 185:2017, commissioned by NPSA, and the NCSC Connected place guidelines provide the necessary inputs for smart service security, CPC-SH2 commented that they do not go down to the level of detail in the same manner as the Manual for smart streets; with case studies for the LAs to

understand how they can be implemented (Transport Technology Forum, 2022; CPNI, 2017; NCSC, 2021b).

DSIT-SH pointed to DCMS survey-based research (DCMS, 2021) that explored what is working well, what challenges exist and what support is required within connected places technologies and ecosystems. PA-SH had the opinion that the PhD research reported here would complement the survey and provide further feedback on the NCSC cybersecurity principles and policies for connected places, to enable them to assist the LAs. DSIT-SH added that those surveyed were consumers of connected place technologies working in local government or other organisations, with the responsibility for the design, procurement, and management of connected places. However, as mentioned by DSIT-SH, the DCMS survey did not include an in-depth analysis of issues faced by the LAs to assess security risks using the NCSC cybersecurity principles for connected places, within the smart service rollouts.

PA-SH and DSIT-SH were keen to understand the initial findings from the stage 2 (second phase of Data gathering) of the researcher's study to support the UK Government's Alpha testing project. The scope of this project was to setup resources by April-May 2023 to help the LAs better implement NCSC cybersecurity principles for connected places. PA-SH and DSIT-SH believed that the findings could help validate the scope of the Alpha testing project. The EV charging use case was of particular interest to the NCSC-SH1, NCSC-SH2, NCSC Energy team and PA-SH.

5.3.1.3 Procurement for smart services

Group 2 were consistent in their responses regarding procurement for smart services. They reported that LAs own / manage the land provided for EV charging stations and are in a unique position to know the demography and requirements of their citizens, and hence they are key players in facilitating smart service infrastructure. The LAs use existing (procurement) frameworks to procure smart infrastructure and associated services. LA-7 mentioned that the procurement frameworks simplify the procurement process for stakeholders and aim to instil confidence in the suppliers by providing the specifications in a template, ensuring compliance with legislation, assisting in qualifying the suppliers against a tender and streamlining the procurement process. The regulatory and legislative security requirements for the smart infrastructure services were also embedded within the procurement frameworks. However, LA-7 raised concerns on operational monitoring for cyber-attacks by providing examples

from other use cases. LA-7 pointed out that any feed from the individual sensors at bus stops and lamp posts are operated by separate organizations and there is currently no other integrated service apart from the applications on mobile phones. The general feedback from all LA stakeholders was that the EV charging service has been procured through good frameworks and could be assessed for security requirements.

5.3.2 Results – Stage2 - Phase 2: General questions

The initial observation from the answers to the five general questions (Table 5.6 A) in the second phase of data collection (among the Group 2 stakeholders) was that the practices followed for the procurement of services and security measures seemed to be consistent. There was full agreement among the eight stakeholders on the roles, responsibilities, accountabilities, liabilities, challenges, and processes that were followed for EV charging operations. The results from the five initial generic questions are outlined below:

1. How are the responsibilities shared between the LA and the CPO for smart service rollouts?

All eight stakeholders gave a consistent response to this question. The LAs retain full ownership of the charging network and enter a fixed term contract with the CPO for operations and the maintenance of charging point services. EV charging procurement contracts include an agreement for a 5% to 15% revenue sharing model with the CPO. Although the LA stakeholders review the performance of the services regularly, the CPOs are accountable, and liable for the secure operations of this service as per their procurement contracts.

The LAs focus on mapping onto the Government's EV infrastructure strategy, planning for the EV charging stations, citizen safety, aesthetics, licence requirements and efficiency of the services. The LAs had developed an EV strategy after gaining an understanding of the market technology availability, delivery models (such as revenue sharing between CPO and the LAs) and specifications. The LAs implement their EV strategy and give the CPOs a contract to install, operate and maintain the EV charging services. As a part of the procurement process, the LAs firm up their specifications as well as assurance questions and evaluate the bids from the charge point suppliers against a range of cost, standards, regulatory compliance, performance of services,

and quality criteria. The selected supplier/suppliers are given the contract to supply, install, maintain, and securely operate EV charging facilities generally for 2-3 years.

2. What is the process of including security and resilience requirements in the procurement contract?

All eight LA stakeholders explained that they use standard procurement frameworks which included the *Go Ultra Low Cities Scheme* (GULCs, a framework developed by Transport for London), the Crown Commercial Service Vehicle Charging Infrastructure Solutions (VCIS) and the Eastern Shires Purchasing Organisation (ESPO). LA-7 mentioned *“The procurement framework is used as a dynamic purchasing system, using a zero-capital delivery model route.”* The example provided by LA-7 was that TfL had added legal and liability clauses, data specifications, pricing strategies, contract terms, requirement for reports and exit clauses on top of the specifications in the procurement framework. LA-7 added *“There is no guidance available for bids that protect the LAs against CPO taking advantage due to them leading on the EV charging solutions. TfL took the role of helping the LAs with the procurement framework and guidance for the tender, as well as the bid pack, to ensure that they are protected from unreasonable specifications put in by the CPO”*. An example was provided by LA-7 where, historically, a CPO had suggested putting in an unreasonable clause in the contract where no other charger could be installed within 2 miles of their charging point.

LA-5 reported that some LAs have developed their own frameworks. Examples included frameworks managed by Kent Commercial Services, the Central Southern Regional Framework, Hampshire County Local authority, and Oxford City Local Authority’s Dynamic Purchasing System (DPS). LAs shared their frameworks with other LAs. The stakeholders could customise their tenders’ using elements of any of these shared frameworks. The LAs also added specifications based on the IT policies within their organizations and the procurement team’s decisions based on collaborative inputs. Additionally, guidance and support were available from multiple sources, such as the Electric Vehicle Energy Taskforce (convened by the Office for Zero Emission Vehicles (OZEV) at the behest of ministers) and local Government support programmes.

The procurement frameworks contained basic requirements for cyber security. LA-3 and CPO-1 felt that the process followed should take sufficient care of the

security requirements. LA-3 said, *“We use our organizational ICT security policies and standard questionnaire to assure the CPO’s services at the time of procurement using approved frameworks.”* LA-6 mentioned that the risk mitigations in procurement contracts achieved the goal of ensuring that the LA is not liable for any operational risk. LA-6 had suggestions about what is required to assure the procurement contracts have adequate specifications for cybersecurity and resilience – *“There is little guidance on which standards need to be complied with for the cyber resilience of the EV charging service. The LAs need to know the implications of a cyber-attack and consequences of not including the standards for cyber resilience.”* LA-5 said that, where there is a potential for cyber-crime, the police need to step up to help. LA-5 added, *“The police could look at potential cybercrimes and provide security interventions to be placed in procurement specifications for connected places based on anticipated crimes. For example, the police have provided the specification for the Modern slavery policy to be placed in all public sector contracts as a requirement.”* LA-7 said, *“It is a good challenge as to whether the cyber security and resilience requirements in the frameworks and bid pack are sufficient.”*

3. Are you aware of NCSC's Connected places guidelines?

None of the eight stakeholders were aware of the guidance within NCSC cybersecurity principles for connected places. The stakeholders shared a common view that the cyber risk associated with the EV charging service needs to be managed by the EV Charge point operator (CPO). LA-6 had joined an initiative called the Transport Technology Forum (TTF) led by The Department of Transport, to work with public and private organizations and facilitate the creation of a guide for the LAs, their officers and consultants planning to implement the Electric Vehicle charging schemes. LA-6 mentioned *“There is too much information out there and it is hard to understand / find relevant information as well as processes. It is tough without a training course for the officers. Also, departments work in silos and processes are not clear to everyone. Therefore, I have taken an initiative within the Transport Technology Forum (TTF) to provide a start-up document for people, processes, roles, and responsibilities.”*

LA-2 had some feedback on NCSC guidelines *“NCSC guidelines are usually not constructive, there is no baseline and there are no checks.”* None of the LA stakeholders were clear about the process of how the new set of guidelines from NCSC can be included in the procurement process. LA-6 added *“There is little*

guidance on which standards need to be complied with for the cyber resilience of the EV charging service. The LAs need to know the implications of a cyber-attack and consequences of not including the standards for cyber resilience. The LAs need outputs from a study of procurement contracts which mention the review points, what is missing, gaps and a full guide for inclusion of standards and requirements. The procurement evaluation matrix to validate supplier capabilities also needs to be a part of this set of documents. NCSC guidelines need to include this information for the LAs to use it.” What LA-4 mentioned was noteworthy - *“There is a language barrier between usual local authority officers and the cyber security area. Using NCSC guidelines to assure cyber resilience is not considered the job of local authority officers in traditional functions such as procurement.”*

4. Are you aware of the potential cyber-crime scenarios for the smart services procured?

The crime scenarios shortlisted from the literature review (see Table 5.2) were discussed with each of the LA stakeholders. All eight stakeholders mentioned that they are aware of cybercrimes in a traditional sense (such as ransomware, distributed denial of service, theft in payment systems). However, none were aware of any incidents where cyber-attacks had disrupted EV charging services, EVs, power grids or any other connected ecosystems. LA-6 commented that *“The cyber risks have been thought through, but not yet experienced.”* LA-2 pointed out that *“the cyber-crimes and security mitigations are limited to IT systems, IoT devices, networks, or physical crimes. The cyber risk analysis conducted by the LAs focused on individual services and products rather than how security measures protect connected places from the crime scenarios presented by you”*. LA-4 also mentioned that *“There is not enough awareness about cyber risks nor has there been any widespread high profile cyber-attack on EV infrastructure, it is considered a low risk and hence it is not on the top of the LA's agenda.”*

5. When you procure smart EV charging services, how do you identify as well as manage the security and resilience risks of connected places?

As none of the LA stakeholders were aware of the NCSC connected place guidelines, the researcher discussed with CPC-SH the key measures used to mitigate the cyber risks for the EV charging case study within the Manual for smart streets.

CPC-SH noted that the LAs follow the IT standards when they procure services and referred the researcher to the Practice Manager for Transport from the Energy Systems Catapult (ESC). As informed by the ESC stakeholder, the UK Government had a security framework and governance in place for the energy sector to protect the electric grid from developments such as EV charging (HM Government, 2022). The researcher was sent a link to the EV Energy Task force, which comprises multiple private, academic, and public sector stakeholders. They published a report in October 2020 with 10 high priority actions, one of which was “*delivering a resilient charging infrastructure*” (Energy Systems Catapult, 2020). The action specifically included “*the implementation of cyber security practices that go beyond the charge point and deliver the required digital infrastructure and appropriate certification schemes*” (Energy Systems Catapult, 2020). This indicated that the required standards for cyber resilience of smart EV charging were in the process of being fine-tuned.

All eight stakeholders had the same view that the cyber risks for EV charging services were managed as per the standards and regulations embedded in the procurement process, which should overlap with NCSC cybersecurity principles for connected places; however, there has been no assessment against NCSC cybersecurity principles for connected places. They also shared a common opinion that the CPOs had their operational risk management as well as resilience processes in place.

These responses were discussed with the focus group. This resulted in DfT-SH2 reporting that in the UK Government’s Alpha Testing project to support the LAs to implement Connected Place guidelines, the scope was being refined to include governance, procurement, and threat assessment support. DfT-SH2 also explained that the plan was to roll this out by Feb-March 2023, including the governance for connected places, data protection impact assessment support, procurement support specific to smart services and threat assessment workshops using the ‘STRIDE’ model (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege).

5.3.3 Results – Stage 2 - Phase 2: Conformance to cybersecurity principles

The researcher reviewed the documented responses to the questions specific to the implementation of each NCSC cybersecurity principle in scope of this study (Table 5.6 B). An assessment of the extent to which the NCSC principles have been embedded

in the current procurement of smart EV charging services in the UK was conducted by comparing the actual measures used by the LAs, based on the information provided by the eight stakeholders, with the published NCSC guidance (NCSC, 2021a). This comparative assessment is explained below. As seen in Table 5.1, principles #6, #7, #8 and, #11 are out of scope and hence are excluded below.

#1 Understanding your connected place and the potential impacts: *The first step is to gain a clear and complete understanding of your connected place goals and ambitions. Who has overall responsibility and accountability for your connected place? What external dependencies does your connected place have on other systems within the street eco system? What is externally dependent on your connected place?*

NCSC Connected Place principle 1 clearly expects that inward as well as outward potential dependencies - as well as impacts within the connected place ecosystem - must be understood (NCSC, 2021a). There needs to be a clear and complete understanding of the connected place goals, ambitions, overall context, and accountable ownership of the connected place (NCSC, 2021a). However, a connected place supports multiple critical functions and services i.e., one or more of CCTV, transport, streetlight management, utilities, and other public services. Hence it is important to analyse the impact of a cyber-attack on multiple critical functions across multiple services in a connected place when introducing a new smart service.

As explained by all eight stakeholders, the LA and CPO roles are limited to rolling out an EV charging network to achieve the targets for EV transition. However, five out of eight stakeholders said that operational security is not assessed beyond the CPO's responses to the assurance questions in the bid pack. LA-7 agreed that *"Analysing the outward dependencies and risks is not prescribed within the procurement frameworks used for EV charging contracts."* LA-4 mentioned that *"In many instances, existing infrastructure/services for legacy EV charging infrastructure are standalone. They are connected much later (after 2 years), and hence external dependencies are possibly not assessed to the required extent."* All eight stakeholders mentioned that any damage during operations is the accountability of the CPO and is covered by liability insurance taken out by CPOs. LA-1 added *"There is less awareness about the connected places ecosystem. Focus is on individual rollouts*

such as Go Ultra-low city scheme for lamp posts, car sharing (as well as mobility solutions) and EV transition.”

The CPO had a view that there was minimum dependency management and risk for EV charging services. CPO-1 reasoned that IT, interfaces, network, and supply-chain dependencies are a part of the design to protect the EV charging service from external dependencies. CPO-1 provided an example *“EV charge points are wired in parallel with streetlights and not integrated with them to protect the connected place. This ensures that if the charge point on a streetlight goes down, the streetlight network is not impacted. The link of EV charging equipment with vehicles is currently a hard-wired connection, there is no electronic / data connection from vehicles to charge points or vice versa and hence it is secure”*. CPO-1 offered an opinion that further protection is expected within individual external systems (e.g., inbuilt protection in the vehicles to prevent overcharging which provides a second layer of protection). However, research shows that cyber breaches have been reported for Direct Current Fast Chargers (DCFC) due to the complexities involved (Hodge et al., 2022). If a cyber-attack on EV charging results in overheating the EV battery, the vehicles do not always have in-built protection. In 2020, due to concerns around EV fires (which are more hazardous than normal fires and need special training to treat the recurrence), Hyundai and General Motors (GM) each had to recall nearly 100,000 EVs (Gear, 2021). Agreement is in progress in the automobile industry on the implementation of fire protection for the EV battery and thermal management for an EV (Gear, 2021). It is now being recommended by Zurich Insurance that a fire risk assessment should be carried out in compliance with Fire safety Regulations, to mitigate the hazards of Lithium-Ion batteries catching fire (Zurich Resilience Solutions, 2021).

There was consensus among all eight stakeholders that not enough thought is being given to the connected place, or the overall potential impacts to the connected place ecosystem each time a specific connected service, such as EV charging, is being rolled out. The stakeholders work on the procurement of individual rollouts and have less awareness about dependencies across networks owned by multiple organizations within connected places ecosystems. LA-2 said, *“City authorities do not analyse the ecosystem. Private operators run the connected place. Not everyone carries out due diligence and projects are not actioned with confidence. The big picture is lost as contract compliance is what remains.”*

To summarise, with respect to NCSC Connected places principle #1, there are gaps in the local authority's procurement processes regarding the assessment of dependencies in the ecosystem. Specifically, there is insufficient analysis of the context and external dependencies to understand the potential security impacts to the ecosystem prior to rolling out a smart service.

#2 Understanding the risks to your connected place: *You need to have a clear understanding of your connected place infrastructure by identifying, understanding, and assessing inter-dependencies. Have you understood the resilience needs, vulnerabilities and threats to connected places? Have you identified risks that you can prioritise according to how concerning they are and what impacts are unacceptable?*

This principle focuses on the need to identify vulnerabilities and threats that could exploit the connected infrastructure and impact the connected place. There is a clear expectation that a formal risk assessment of the link to the connected place ecosystem and ongoing risk management by the owners of the connected place has been carried out. The LA stakeholders believe that it is the CPO's responsibility to manage threats, vulnerabilities, and risks to their services. Due to a lack of skilled resources in the LAs, the concessionary arrangements (to develop, operate and maintain an infrastructure asset) are put in place with the help of suppliers who are experts in the area. The LAs are aware of cyber risks in terms of customer data leaks, denial of payment service, theft of charging cables, and ransomware attacks. Hence the procurement specifications include regulatory requirements such as General Data Protection Regulation (GDPR).

However, the risks are not assessed from the lens of potential cyber warfare threats affecting the ecosystem through the EV charging service. For example, in Feb 2022, after the invasion of Ukraine by Russian forces, hackers disabled EV charging stations on the 450-mile highway between Moscow and St Petersburg (Jeffay, 2022; Malik & Anwar, 2022; Plaka et al., 2023; Skarga-Bandurova et al., 2022). LAs were not aware whether the cyber resilience measures are adequate to prevent such an attack. Another threat scenario was discussed wherein a hostile nation could gather information through the CCTV network in an EV charging station and attack transport, a CNI through a vulnerability in the EV charging infrastructure. All eight stakeholders agreed that the vulnerability or threat assessment is not done through the lens of such

scenarios. LA-2 believed that *"The cyber risks are not thought through in the manner that you have described. Utter ignorance on the subject is phenomenal"*.

The LA professionals depend on regular guidance on updates to the procurement frameworks, knowledge within their teams and from collaborative efforts to ensure that relevant risk mitigations are embedded in the contracts with the CPOs. According to LA-3, *"The key mitigation measure for the resilience of the EV charging service is that procurement contracts are given to more than one CPO. So, if the services of one CPO are not available, there is an alternative available to the users."* LA-6 pointed out *"The risks are analysed and built into the bid pack based on the experience and knowledge of the bid manager."* Seven out of eight stakeholders mentioned that collaborations are being developed across the LAs, to learn from each other and reduce the risk of exposure. LA-6 mentioned that *"I am leading on a DfT initiative within the TTF to help the LAs share the specifications and methods for creating the procurement contracts."*

All stakeholders stated that the private operators are expected to lead on the threat, vulnerability, and risk assessments for the smart service network they provide. CPO-1 reported that they have robust processes in place for the threat and vulnerability assessments. Further discussions revealed that the CPO leads on doing mainly IT focussed risk assessments through the lens of organizational systems and networks (e.g., accessibility, data protection, network protection and GDPR). CPO-1 explained that *"Currently, risk analysis includes potential basic crime risks such as the duplication of Quick response (QR) code (an optical bar code available on a mobile phone that links to various online functions such as contactless payment), credit card fraud, data leakage and petty theft."* CPO-1 had an opinion that security is also built into their design decisions such as the use of open-source protocols (considered more secure than other protocols), secure handling of customer information associated with Radio Frequency Identification (RFID) cards, reading energy demands, minimal low risk information in exchanged messages and no transfer of data between an EV charge point and vehicles limit the risks to EV charging services.

To summarise, partial gaps were found in the LA's procurement processes when assessed for conformity with the NCSC Connected places principle #2. All the LA stakeholders who participated in the study conceded that in general the CPOs engaged by them had more knowledge in this area, and they assess cyber risks regularly to some extent. However, the LAs do not assess cyber threats,

vulnerabilities, and risks in the ecosystem within the procurement process from the lens of preventing high-profile cyber-attacks critically disrupting EV charging services, EVs, power grids or any other connected ecosystems.

#3 Understanding cyber security governance and skills: *Your connected place cyber security needs to be owned, governed, and promoted at the top level of the organisation. This accountability cannot be outsourced to suppliers. Do you own and govern the risk structure for both service resilience and user privacy? Do you have the right security, business, and technical knowledge to enable them to make effective and timely risk management decisions? Does the connected place have the resources and funding available for its upkeep such as operational security and improving future services and building new capabilities in line with technological advances?*

As stated by all eight stakeholders, the CPOs contractually own, govern and are liable for the performance as well as associated security risks of the EV charging service operations throughout the whole system life cycle. As LA-6 explained *“The LAs do not have any liability for security breaches of smart services. As an analogy, the LA gives a car park on lease to operators. If a car gets vandalised in the parking, the local authority does not have any liability.”* If there is an impact to service availability or reliability due to a cyber-attack, the CPO could be facing financial or other contractual implications. They added that, unlike the CPO, the LAs do not have the skills to assess the security of the services or the business, and technical knowledge to make effective and timely risk management decisions. LA-2 had an opinion that *“The consequence of the LAs not being fully liable for cyber security of services is that the impact to end users is not thought through by everyone.”*

The principle also states that the connected place must have the resources and funding available for its upkeep, such as operational security and improving future services in line with technological advances (NCSC, 2021a). All stakeholders noted that the LAs upgrade contracts every 2-3 years to embed technological advances, funding for the upkeep of EV charging stations and the improvement of services (includes supply-chain). However, the LAs do not govern the risk structure for service resilience within the connected place, other than by putting stringent service performance requirements on the CPO and analysing them regularly. CPO-1 agreed with the LA stakeholders *“the governance of operational security, embedding*

technological advances, funding for the upkeep of EV charging stations and improvement of services (includes supply-chain) are a part of their contract and a responsibility that is key to our business interests.”

The risks and liabilities are shared between the CPOs and its supply-chain, whereas the LAs focus on transferring the liability risk within individual rollouts (such as EV charging) of a connected place. Through the life cycle of EV charging operations, the CPO and its main supplier audit each other; however, the LAs do not audit the CPO, nor do they check/ assure what is being delivered post contract award. As mentioned by CPO-1, *“With our partners it is more of a business contract; with the LAs, not so much”*.

LA-4 explained that the technological advances that improve future services are covered through improved procurement frameworks and enhancements made by CPOs to their services. LA-1 mentioned that *“Horizon scanning is carried out as and when seen fit. Public sector organizations either renew the contracts or change the supplier every 2-3 years.”* LA-4 added *“The renewal / new bid includes requirements specific to technological advances, future proofing needs and new legislations.”* Examples provided by LA-4 included updated / new contracts for EV charging stations being upgraded with connected infrastructure, advancement of rapid charging, and more interoperable solutions offered by suppliers. Another example was cited by LA-4 *“the LA is deploying 5G network and now we are analysing future impacts of too much reliance on city data store outputs.”*

To summarise, the assessment of NCSC Connected places principle #3 revealed gaps in the ownership of cyber threat governance by the LA. The resources and funding required for the upkeep, improvements and building new capabilities for EV charging services is managed by the LAs. However, although the service performance is governed by the LA, the service resilience risks due to the cyber threats for the connected place ecosystem are not owned and governed at the top level of the organisation. The lack of skilled resources in the LAs is one of the causes for the lack of governance discussed.

#4 Understanding your suppliers' role within your connected place: *You cannot outsource your accountability to your suppliers, as you are the overall risk owner for your connected place. Do you consider your suppliers' roles as part of your overall risk management governance process in building and operating your connected place?*

What assurance requirements are built into your connected place supply chain, and how these are going to be reported to you and your suppliers? For example, what is the plan to deal with the risks to connected place ecosystem and its services due to a supplier taken over by a foreign corporate group? How your suppliers will report any suspicious or malicious activity and assist you when needed.

This principle reiterates that “You are the overall risk owner for your connected place. You need to consider the role your suppliers have in building and operating your connected place. You should incorporate your suppliers' roles as part of your overall risk assessment process. There may be areas of split responsibility within your connected place that you may have with your suppliers, but it is still up to you to make sure the supplier fulfils this (NCSC, 2021a).” Amongst the list of what needs to be included, the guidance specifically mentions that the assurance requirements need to be built into the connected place supply chain, and how these are going to be reported (NCSC, 2021a).

LA and CPO stakeholders reiterated that the overall security risk management governance process involved in building and operating the connected place are limited to assurance questions in the procurement bids about (i) compliance with security standards, (ii) self-declarations provided by the CPO as responses to assurance questions and (iii) the performance metrics defined during procurement being reported by the CPO during operations. None of the seven LA stakeholders saw the need to create any assurance mechanism to check whether a CPO is prepared for a cyber-attack and manages the continuously developing operational security risks regularly. They believed that if the risks are not managed, it will impact the service performance which is being monitored by them. So indirectly, this mechanism would work as an assurance mechanism to some extent. LA-1 explained that *“Ongoing assurance is not featured as a problem for contract management. Hence, the norm is to procure a CPO that qualifies through framework, defined quality criteria/checks and passes capability assessment. All concessionary contracts are subject to assurance mechanisms. But the cyber security requirements are not assured ongoing and are limited to the bid pack”*. LA-4 mentioned *“The in-depth thinking on cyber risks is starting to emerge due to the target of 95% availability of services.”*

CPO-1 mentioned that they assess their supply-chain risks, carry out assurance checks regularly, and their back office was 100% auditable. When asked about the

contract with the LAs, CPO-1 responded by saying *“The LAs have processes for their contracts; however, they do not have the ability to check on what is being delivered.”* The lack of skills, expertise, and capabilities to carry out assurance was echoed by all seven stakeholders from the LAs. LA-7 stakeholder made an important point that *“the LAs are not aware of what they need to ask for fool proof solutions. EV charging rollout should be managed at Government level rather than the LAs learning from each other.”*

In response to the question about a supplier engaged with the CPO being taken over by a hostile foreign group, the LA stakeholders believed this is a real risk despite stringent supplier assessments being carried out prior to contract award. LA-4 commented *“We need to think about the implications of the 5G network and reliance on data being ingested from connected infrastructure across the city. The latter helps us understand how the city operates, and we are exposing ourselves to the risk of this information being used by hostile actors.”* All eight stakeholders noted that there is no mechanism for the LAs to have visibility of the CPO’s supply chain (insider threats), as it is an internal issue for the CPO to manage. Although procurement frameworks and city authorities have measures in place to ensure that a contract is not given to a banned supplier, there is a risk of a weak measure or insider threat could lead to a deal with an unethical company or supplier that has links with hostile countries.

All eight stakeholders explained that supply-chain risks are analysed by the LAs through vetting processes in their procurement framework before qualifying CPOs for the bid. LA-6 added *“Finances, background, and company house checks mandated post Brexit are in place”*. LA-4 raised a concern that *“A hostile country/ actor could acquire all types of data about locations, processes, and people using various methods.”* LA-2 raised an issue that this process is not fool-proof, and the question remains as to how the LAs can check whether they are dealing with ethical companies or suppliers that have links with hostile countries. He gave an example of an instance where the procurement framework vendor list included a supplier named Hikvision that was banned in Australia and Europe. LA-2 said *“A quick google search showed serious questions / concerns about working with this company. At the time their partnership with a Scottish Local authority was being sued by residents. So, what I would say is gut / careful checking matters and don't just blindly follow the supplier is 'on a framework therefore safe!'”* LA-2 added that there is concern around human error as well, *“In one instance, facial recognition was left turned on. A lot of data about the*

location and people could have been gathered by adversaries e.g., racial profiling of ethnic groups within the population (a hostile country's interest)".

To summarise, an assessment of NCSC Connected places principle #4 against the LA's procurement processes points to a lack of assessment of maturity for cyber resilience and supply-chain (insider) threats. The LAs do not have the skills or assurance processes within contract management to ensure the full cyber resilience assessments are specified and reported. The private organizations such as CPOs lead on the cyber risk management for their services. The maturity of the CPO's security protections during service operations are not governed by the LAs. The LAs also lack visibility of any assessments of supply-chain insider threats (such as remote takeover by a hostile nation) within the connected place ecosystem.

#5 Understanding legal and regulatory requirements: *Do you ensure that the data architecture of your connected place infrastructure is built and configured to fulfil the regulatory requirements set out in the GDPR and the Data Protection Act 2018? Do you also consider any future legal and regulatory requirements that may currently influence your connected place?*

This principle mentions three key regulatory compliance needs – the GDPR, the Data protection Act 2018, and the Network and Information Systems (NIS) Regulations 2018. For EV charging, as mentioned by all eight stakeholders, the procurement frameworks allow the LAs/CPOs to assess the data protection implications and compliance with GDPR amongst other standards, as well as regulations. As noted by CPO-1 *"Smart charging is supported by standards such as electric standards, communication standards and interoperability standards. GDPR and public data protection are amongst the most stringent assurance requirements in public tenders."* The LAs include requirements for regulatory compliance in a bid and the CPO's responses are accepted on trust. The NIS regulation that takes care of cyber risk assessment is not mandatory for EV charging services. LA-7 added, *"The LAs are adding more compliance standards in the future contracts as they learn about them."*

To summarise, no gaps were found during the assessment for NCSC Connected places principle #5 against local authority's procurement processes.

#9 Design your connected place to be resilient and scalable: *Planning needs to be part of your connected place's design, to allow for your systems to be easily scaled, and resilient to attack. Do you define acceptable levels of service, requirements for resilience to attacks and the speed at which the system should scale to meet any increased demand?*

This principle focuses on resilience, scalability, and acceptable levels of service (NCSC, 2021a). As mentioned earlier (Discussion of responses to General Question 2 and principle #1 above), procurement bids may not receive adequate evaluation of the cyber resilience of EV charging smart services; CPOs lead on building resilience by design and any impact to the services due to cyber issues are owned by the CPO. All stakeholders also mentioned that the interoperable physical design, upgrades, and scalability requirements are a part of procurement contracts. LA-2 provided an example that in three west London boroughs, the capacity of the grid to provide EV charging stations has been reached, hence, there are no further expansions planned for the EV charging network until electricity sub-stations are upgraded. CPO-1 raised an important point *"The cloud-based server system has long term scalability for future smart charging options. However, CPOs do not have awareness of everything that is going on in the industry. Currently the vehicle industry is strong arming the EV network but, the vehicle network could be deficient. It is a task to understand whether EV networks are evolving in sync with other networks. There is a risk that smart charging is not mature for the long-term evolution of mobile data network. City authorities accept the technology, the buck stops at the customers (i.e., consumers of the services)."*

All eight stakeholders reiterated that acceptable levels of service performance are defined, monitored, managed, reported, and assured in the procurement process. However, LA-7 raised a concern that *"The Service Level Agreements (SLAs) are built for traditional service operations (such as availability, reliability) with quick fix to mechanical faults in mind, not cyber-attacks."* LA-1, LA-5 and LA-6 mentioned that the procurement requirements are updated based on collaborative improvements across the LAs. LA-7 said *"TfL has progressed and taken 2 years to collate the guidance, but the cyber security view is relaxed as it is not seen as a risk. Sometimes there is a long wait for resources who can write proper bid documents as skilled*

resources are not easily available. Procurement personnel keep changing and hence it is difficult to mature the procurement requirements.”

To summarise, it was observed that the scalability, resilience, and acceptable levels of service are in place to some extent and are continuously improving. However, the cyber risk metrics are not reported by the CPOs to the LAs. There are no checks to understand whether a) the service performance metrics are adequate to understand the cyber threats in connected places, and b) requirements for resilience used by the CPOs are adequate.

#10 Designing your connected place monitoring: *Your monitoring design should give you visibility of all aspects of your connected place system, including endpoints and network edge devices. Is the connected place monitoring system independent from the operational connected place systems? Is the baseline view of the normal cross-service operations across the supply-chain of connected place created and monitored to identify anomalies and report as well as assist in resolving suspicious activities. Is your supplier actively monitoring and reporting the threat landscape and adjusting the protections that they have in place to deal with these threats?*

This principle states, amongst other requirements, that the “monitoring design should give you visibility of all aspects of your connected place system, including endpoints and network edge devices. As threats and technology evolve, so must your monitoring and event selection, which will enable wider visibility of your system (NCSC, 2021a).” All seven LA stakeholders mentioned that although they are aware of monitoring for changes to the threat landscape and cyber anomalies, this is not a part of procurement contract requirements. They believed that monitoring platforms and the emerging threat landscape is an implicit part of the CPO’s service delivery. LA-1 said, *‘Whether the connected place monitoring system is independent from the operational connected place systems’ is not something a local authority would ask a CPO, as it is their job to monitor the security of their services.* LA-3 and LA-5 mentioned *“The LAs only ask for declaration of compliance to cyber security standards from the CPO.”* LA-6 also mentioned that *“CPOs are not asked about threat assessment or the design of operational monitoring as they manage it internally with their suppliers. It is assumed that CPOs follow standard monitoring processes. The LAs are not experts in this area”.* LA-4 added *“Cyber risks, if monitored are not*

reported to the LA. The local authority does not have skilled resources to assess anomalies which is anyway the responsibility of the CPO". LA-2 also mentioned the lack of awareness within the LAs of how monitoring needs to work and the details. LA-2 added *"It is the seller's market. Too many requirements are seen as a roadblock to securing a CPO. The LAs chase the same supplier putting them in the position of power."* CPO-1 agreed that monitoring their IT estate within their network, anomaly detection, risk assessment and adequate response were a part of their service operations and business contracts with their supply chain. CPO-1 said *"The monitoring systems being independent from the operational connected place systems should be a part of the operational design. The server mechanism is subject to continuous risk analysis and monitoring. IT provides 24/7 responses to alerts to limit risks. We resolve suspicious activities as well as adjust the protections. There is a dedicated cybersecurity team. We share risks and liabilities across the supply-chain."*

The principle also states that "Within your monitoring design, you should include the visibility of interconnected systems, sources, and cross-service areas, remote access, and connection attempts. Depending on your connected place, this could include data from traffic lights, streetlights, CCTV systems, parking sensors, pollution sensors, noise sensors, and other IoT devices that are part of your connected place infrastructure where these components produce security events or logs (NCSC, 2021a)." All eight stakeholders agreed that there is no clear definition of who can be assigned this role of designing and managing the monitoring of alerts across the connected place infrastructure. LA-7 raised a concern that *"There is a challenge in monitoring the threat through software alerts across connected place services owned by multiple organizations. They monitor their servers, but it is very complex for any one organization to analyse all monitoring anomalies /alerts to make sense of any threat to the connected place."* CPO-1 added *"Monitoring depends on the ownership of the platforms. For example, CCTV network, vehicle network and EV charging network are monitored by different operators. The anomalies when joined up across these networks could possibly provide risk triggers."* LA-7 explained the concept further with the example of a smart bus stop, where multiple services such as schedule display, digital adverts, CCTV, and ticket vending machines are run by multiple operators. *It is incredibly difficult to get a view of, and join up, the anomalies noticed by the individual operators, to get a clear picture of the threat.*

To summarise the results of assessment of NCSC Connected places principle #10 against local authority's procurement processes, it was found that there was lack of ownership for continuous threat monitoring across the connected place ecosystem. *The services in the connected place ecosystem span multiple organizations and multiple dependent networks, operating under multiple procurement contracts. Due to the inherent complexities involved, the anomalies within individual networks are not joined up to provide risk triggers for the connected place ecosystem. LAs do not have the visibility as to whether the security protections are adjusted by the CPOs based on the changing threat landscape.*

#12 Managing your connected place's supply chain: *Supply chain controls need to instil confidence and trust to ensure your connected place has the right levels of protection. Have you established a minimum set of cyber security and functionality expectations and hold your suppliers to account contractually throughout the whole system life cycle? Has the LA and the operator performed risk assessments to understand the supply-chain risks? Do you have the mechanisms (or criteria) to check that the protections your supplier has in place meet the level of security required for your connected place? Do you implement the 'right to audit' into all contracts and exercise this?*

This principle focuses on “*Supply chain controls need to instil confidence and trust to ensure your connected place has the right levels of protection. You have clarified with your supplier what level of security is required for your connected place. You can do this by establishing a minimum set of cyber security and functionality expectations and hold your suppliers to account contractually. If the CPO's security performance drops, there is an expectation of immediate upward reporting to the LAs. You have the mechanisms to check that the protections your supplier has in place meet the level of security required for your connected place. You should implement the 'right to audit' into all contracts and exercise this. You should encourage your supply chain to consistently improve its security hygiene (alongside your security requirements) to deal with the same sort of threats that constantly lead to issues such as malware or ransomware (NCSC, 2021a)*”.

All seven of the LA stakeholders reiterated that security and resilience requirements were already mentioned in the bids and that security levels were

monitored through service performance reports during operations. LA-7 expanded on this, saying *“Procurement frameworks have limited inputs on cyber resilience specifications and the LAs do not have full understanding of what cyber risks need to be assessed in the procurement stage. Due to lack of expertise in the cyber resilience area, the LAs depend on private organizations to lead the way for what functionalities can be provided with minimal risk and be accountable for cyber risks of their services. Rather than a formal risk assessment, questions are asked to the suppliers and the reply becomes a part of the contract.”* LA-7 added a concern that *“. The requirements for cyber resilience are inconsistent across public sector organizations.”* Although the ‘right to audit’ is a part of the contract, the LAs do not have the capabilities to conduct an audit or understand the reports if sent by the CPO. CPO-1 reiterated that they manage the service risks effectively within their supply-chain, but that there is no assurance process within the LAs to verify that the connected place has the right levels of protection. CPO-1 said, *“Any improvement in security is driven by changes to procurement contracts or security standards that the CPO complies to.”* CPO-1 also made a comment that it will help if all compliance requirements demanded by the LAs from them also cascade to the LAs.

To summarise a) the requirements in the procurement contracts may not cover adequate and consistent cyber security requirements in the procurement bids, b) the CPO leads on the cyber risk assessments for the supply chain for which the LA has no visibility and, c) the LAs do not exercise their ‘right to audit’ for cyber resilience of the smart services.

#13 Managing your connected place throughout its life cycle: *Your supplier supports your connected place throughout its lifetime. How readily you can change suppliers, should the need arise, and the level of support required to do so? How do you test your systems throughout their lifecycle to assure required security levels?*

This principle mentions the need for “clear responsibilities, processes, and procedures in place throughout the connected place’s life cycle to assist stakeholders, vendors and integrators in delivering evolving requirements.”

All eight stakeholders provided inputs that were similar. The term for CPO contracts is usually 2-3 years for EV charging services. Due to opensource and interoperable designs, risk assessments and multiple background checks, supplier

contracts have been quite robust. The LAs have terms covering the right to terminate a supplier if there is a breach of contract. LA-1 said *“Changing suppliers is not known to be an issue. A supplier going bust is also not an issue as the other operators in the market take over the charge points, decommission the infrastructure, recycle it and install new equipment as required.”* CPO-1 said *“Incorporating technological advancements is in a CPO’s interest. The tenure of the contracts being 2-3 years also helps incorporate changing industry demands.”*

This principle also states that “You need to understand the impact of the components to your connected place, and that you have effective assurance in place that components are still meeting the required security levels needed to protect the system. You can do this by testing your system throughout its life cycle.” All eight stakeholders mentioned that the LAs include the requirements for security and ongoing security testing in the bid. CPO-1 stakeholder pointed out that *“Security testing is a part of the operational process. We test our systems throughout its life cycle. CPO can change supplier if any contract terms are breached.”* LA-7 added that *“Testing a system through the lifecycle is a requirement in the bid, but the LAs do not conduct ongoing assurance.”* All eight stakeholders were of the opinion that it is left to the CPO to maintain these in a way that they do not impact service performance. LA-7 also mentioned that procurement professionals would need detailed guidance within this NCSC principle to embed it into their tenders.

To summarise, the LA's procurement processes include the right level of support from the CPOs for connected places throughout its lifecycle as required in the NCSC Connected places principle #13. The security levels are tested by the CPO with their supply chain, but they are not reviewed or assured by the LA once the contract is awarded.

#14 Managing incidents and planning your response and recovery: *Connected places should be demonstrably resilient. How is the following handled across various operators and supply-chains?*

- a) *Building a cyber security incident response team (CSIRT)*
- b) *Acceptable levels of service*
- c) *Incident management, response plan and recovery of services*
- d) *Accountabilities and liabilities*

Note: Is there any dry run or walk through of recovery process in place based on lessons learnt or otherwise?

This principle focuses on the planning, detection, response, and recovery aspects to effectively manage incidents such as loss to a critical public service in the event of a cyber-attack. For detecting incidents, the principle specifically states that *“You need to have a wide variety of methods for detecting incidents. This could include third parties such as partners, suppliers, private companies, or the public performing incident investigations and threat research”* (NCSC, 2021a).

All eight stakeholders had similar views and reiterated that the Incident management service levels are a part of the defined service performance levels set out in the contract specifying time frames in which issues should be resolved, this includes cyber-attacks. LA-6 mentioned *“Operational risks are managed by the operator. The LAs don’t share risks with the CPO.”* LA-4 added *“We do not have skills or resources to get involved.”* The management of incidents and plans for response and recovery are handled across the operators and supply-chain as follows:

- a) Building a cyber security incident response team (CSIRT): All eight stakeholders mentioned that this is the responsibility of CPO. CPO-1 explained that they have strong IT and operations teams that have the skills to respond and recover from failures within their networks with cooperation from their supply-chain. LA-7 mentioned *“CSIRT is limited to ownerships of networks, systems, and components which may or may not cover an end-to-end service.”*
- b) Acceptable levels of service: As mentioned earlier in this section, these are defined in procurement contracts and reported by the CPO to the LA regularly.
- c) Incident management, response plan and recovery of services: All stakeholders believed that this falls under service continuity and are a part of the CPO’s contractual responsibility for the EV charging service. LA-7 clarified that *“Any impact of an incident to places or part of services outside their network is not the CPO’s accountability and not a part of their contract”*. All LA stakeholders agreed with this statement. CPO-1 explained that their office had a ransomware attack on the IT systems in the past year due to a server not using the right version of the operating system. It was noticed quickly and resolved with minimum damage. CPO-1 mentioned *“In the event of an incident, hourly updates are provided to the*

LA and any other stakeholders. If the cyber- attack spreads across services outside the CPO's network in the connected place, it is not clear how the prioritisation works for the recovery, however, it is supported by the CPO on a good-will basis (if there is a need)."

As a response to further questions, CPO-1 agreed that the disaster recovery, service continuity and business continuity plans have not been analysed for against a full-fledged list of potential cyber-attacks that were listed by the researcher. As a result, even if CPO leads on it, there is limited assessment on what specifications can be included in the procurement phase to prepare for a cyber-attack that can spill over to the connected place ecosystem. With regards to recovery planning within contractual agreements, LA-2 opined that *"It is not done in a structured manner across the LAs"*.

d) Accountabilities and liabilities:

The common message from all stakeholders was that Incident management, response, recovery, and dry runs are the CPO's responsibility and liability. LA-6 responded by saying that *"The LAs play the role of a coordinator to provide updates if a public service is impacted. Impacts to connected places are not analysed across services in a connected place as the LAs do not have resources or knowledge on this topic."* CPO-1 had the view that *"In event of a cyber incident, as first responders, the local authority's role is limited to providing updates to citizens and Government from the CPO's reports."* LA-2 mentioned that *"although the LAs are the defined first or second responders, they do not get involved in the planning or review of incident response, for example, if there is a ransomware attack that spreads across a connected place, how will it be resolved."* LA-7 mentioned that *"In event of a physical disaster such as a vehicle hitting a charger, whichever organization professional is first on the site (National grid, CPO, supplier of CPO) needs to take measures to keep the site secure. The processes are well defined for physical incidents."* When a specific question was asked about the local resilience forums to LA-2 and LA-7, the response was that they do not get involved in the review of cyber incident management plans during procurement; other stakeholders agreed with this statement.

All eight stakeholders acknowledged that contractual agreements do not include questions specific to dry runs for the recovery of services (which would

provide a demonstration of resilience in the event of attacks such as ransomware).

LA-6 mentioned *“So far, the LA has not requested a recovery plan from the CPO through their tender documents as recovery from cyber-attacks is the CPO’s responsibility and the local authority does not get into how they carry out service continuity planning”*. CPO-1 said that they conduct dry runs but not for detailed cyber-attack scenarios. The CPO stakeholder mentioned that they had experienced cyber-attacks and implemented lessons learnt. However, CPO-1 added *“lessons learnt are not always shared with the industry.”* LA-1 said, *“Resilience tests should happen within the LAs across London through coordination in future.”*

In late 2022, LA-7 informed that, *“the council has now included in their current tender that the CPO’s should submit a service continuity plan which should also include submitting a recovery plan.”*

To summarise the assessment of NCSC Connected places principle #14 against local authority’s procurement processes, it was found that CPOs are accountable for the management of incidents and, they are held to account by the city authorities through the contract for networks owned by them. However, the LAs do not have the clarity of how the recovery process works for multiple services in the connected place ecosystem, nor are they engaged in detailed resilience and recovery tests. The LAs do not assess whether the services in the ecosystem are resilient in the event of attacks such as denial of service. It is assumed that the service operators lead on any cyber incidents across the ecosystem. Local resilience forums, the Category-1 disaster responders in event of a disaster, are not involved in providing inputs to build recovery tests/plans for the connected place when a service such as smart EV charging is outsourced to private suppliers. The LAs and CPOs are not necessarily aware of lessons learnt on cyber resilience in the industry.

5.3.4 Summary of Results - Discussion

The initial discussions with the stakeholders in the first phase of data gathering pointed to the fact that although the principles and standards for resilience and security of connected places have been defined, the policies, standards and guidelines are under development or yet to be implemented. These conclusions were supported by an analysis of the documents and links provided by the stakeholders which suggest that the efforts are ongoing across public, private and Government sectors to mature the security and resilience standards for smart infrastructure. The organisations with

responsibilities for providing the guidance for the security and resilience of connected places are working with the LAs to support the implementation of NCSC cybersecurity principles for connected places. However, there was no in-depth study conducted on whether the NCSC cybersecurity principles for connected places were used by the LAs to assure the security and resilience risks during the procurement of smart services. The EV Energy task force stated in Oct 2020 that cyber security practices within the connected place need to be prioritised in order to develop a resilient EV charging infrastructure (Energy Systems Catapult, 2020). NCSC and DSIT are organising initiatives to ensure that the NCSC cybersecurity principles for connected places are understood, implemented, and governed by the LAs. This clearly points to the fact that, although there is a gap in the current security landscape in areas such as cyber risk management in connected places, the Government is working with the private sector to provide the necessary support and encourage resolutions.

The second phase of data gathering pointed to the fact that the stakeholders from the LAs were aware of the smart service procurement mechanisms; however, they were not aware of the threat landscape and cyber risks to smart services such as EV charging (where a cyber-attack can critically disrupt EV charging services, EVs, power grids or and other connected services in the ecosystem). The LAs rely on procurement contracts to provide the standards and were not aware of the NCSC Connected place guidelines. Additionally, they do not have the resources or skills to map the procurement specifications to the NCSC Connected place guidelines, and there is a lack of benchmarks for specifying cyber resilience requirements in the procurement contracts. The LAs do not feel accountable for cyber risks of smart services and the connected place ecosystem. As a result, there seems to be a lack of governance as well as a lack of assurance of cyber risks, and a high dependency on CPOs leading on the security and resilience for the EV charging services. This also conflicts with the Local Government Association (LGA)'s procurement guide that advocates managing the procurement contracts as projects, "incorporating risk management and assurance reviews" (LGA, 2019).

A summary of the results specific to the conformance to NCSC Connected place principles within the LAs' procurement process is shown in Table 5.7.

Table 5.7 Non-conformances: Local authority' procurement process and the NCSC cybersecurity principles for connected places

NCSC Principles	Non-conformance to NCSC Connected place principles within the LAs' procurement process
#1 Understanding your connected place and the potential impacts	Assessment of dependencies in the ecosystem: Insufficient analysis by the LAs for the context and external dependencies to understand the potential security impacts to the ecosystem prior to rolling out a smart service.
#2 Understanding the risks to your connected place	Cyber threat, vulnerability, and risk assessments: The LAs do not continuously assess cyber threats, vulnerability, and risks in the ecosystem within the procurement process from the lens of preventing any high-profile cyber-attack critically disrupting EV charging services, EVs, power grids or any other connected ecosystems. The private organizations such as CPOs lead on the cyber risk management for their services.
#3 Understanding cyber security governance and skills	Ownership of cyber threat governance: Although the service performance is governed by the LAs, the service resilience risks due to the cyber threats for the connected place ecosystem are not owned and governed at the top level of the organisation. Lack of skilled resources in the LAs is one of the causes for lack of governance.
#4 Understanding your suppliers' role within your connected place	Assessment of maturity for cyber resilience and supply-chain (insider) threats: The maturity of the CPO's security protections during service operations are not governed by the LAs. The LAs also lack visibility of any assessments of supply-chain insider threats (such as remote takeover by a hostile nation) within the connected place ecosystem.
#5 Understanding legal and regulatory requirements	None
#9 Designing your connected place to be resilient and scalable	Reporting of cyber risk metrics: Cyber risk metrics are not reported by the CPOs to the LAs. There are no checks to understand whether a) the service performance metrics designed for mechanical breakdowns are adequate to understand cyber threats in connected places, and b) requirements for resilience used by the CPOs are adequate.

NCSC Principles	Non-conformance to NCSC Connected place principles within the LAs' procurement process
#10 Designing your connected place monitoring	Ownership for continuous threat monitoring: The services in the connected place ecosystem span across multiple organizations and multiple dependent networks, operating under multiple procurement contracts. Due to the inherent complexities involved, <i>the anomalies within individual networks are not joined up to provide risk triggers for the connected place ecosystem. LAs do not have the visibility as to whether the security protections are adjusted by the CPOs based on the changing threat landscape.</i> There was lack of ownership for continuous threat monitoring across the connected place ecosystem.
#12 Managing your connected place's supply chain	Cybersecurity requirements, supply-chain risk assessments and 'right to audit': There is limited understanding within the LAs as to whether the security levels of the smart services are sufficient to maintain the required security levels of the connected place ecosystem. Additionally, a) the requirements in the procurement contracts may not cover adequate and consistent cyber security requirements in the procurement bids b) the CPO leads on the cyber security cyber risk assessments for the supply chain for which the LA has no visibility c) the LAs do not exercise their 'right to audit' for cyber resilience of the smart services.
#13 Managing your connected place throughout its life cycle	Security levels not assured during operations: The security levels are tested by the CPO with their supply chain, but not reviewed or assured by the LA once the contract is awarded.
#14 Managing incidents and planning your response and recovery	Lack of resilience tests and dry run requirements: The LAs do not have the clarity of how the recovery process works for multiple services in the connected place ecosystem, in the absence of detailed connected service resilience/recovery tests. The LAs do not test whether the services in the ecosystem are resilient in the event of attacks such as denial of service. It is assumed that the service operators lead on any cyber incidents across the ecosystem. Local resilience forums are not involved in providing inputs to build recovery plans and/or dry runs for the connected place when a service such as smart EV charging is outsourced to private suppliers. The LAs and CPOs are not necessarily aware of lessons learnt on cyber resilience in the industry.
LA – The LAs, CPO – Charge Point Operator	

The LA stakeholders expressed a need for additional support to help them navigate through an overwhelming number of guidelines in the industry and to create appropriate specifications in the procurement contracts. A gap in the cyber resilience of the EV charging smart infrastructure was already identified by the EV Energy task force in 2020, and it is also taken onboard as a priority within the Government initiatives. These non-conformances (gaps) were discussed with the focus Group and shared with the stakeholders involved, for their feedback.

5.4 Results from Stage 3 (Further Analysis)

The data analysis was conducted in three steps. Initially, the guidance provided in the NCSC cybersecurity principles for connected places was critically analysed (Section 5.4.1) to understand whether the guidance, if followed can resolve the non-conformances in the LA's procurement process. A thematic analysis (Section 5.4.2) was then conducted to understand the gaps by identifying similar themes in the procurement process. Finally, a root cause analysis (Section 5.4.3) was conducted to investigate these gaps and to understand the underlying causes. The data analysis was presented to the focus group to seek expert advice prior to finalising the results.

5.4.1 Critical assessment of NCSC guidance

The gaps in the LA procurement processes from Table 5.7 were analysed against the detailed guidance within the NCSC cyber security principles for connected places (see section 5.3.3). The results from this analysis found potential gaps/enhancement opportunities for NCSC cybersecurity principles for connected places. This analysis was discussed with the focus group and adjustments were made based on the suggestions where there was consensus. In the text below, each of the principles are critically assessed. As seen in Table 5.1 NCSC principles #6, #7, #8, and #11 are excluded from the scope of this study and hence are not included below. There were no gaps found for NCSC Connected places Principle #5 (see section 5.3.3) and hence it is also excluded from the assessments below.

Assessment of Principle #1 Understanding your connected place and the potential impacts:

There is a lack of guidance within this principle as to how the external dependencies and the impact on the connected place ecosystem can be assessed when a new service is introduced, or a legacy service is changed to a smart service. NCSC expects a reasonable level of understanding and hence has published only seven sample questions specific to analysing dependencies for a smart service network owned/governed by a supplier under this principle.

Assessment of Principle #2 Understanding the risks to your connected place

This principle could provide detailed guidance to help authorities conduct cyber risk assessments for smart services and analyse how cyber risks could develop into a systemic event within a connected place ecosystem. Additional guidance is required

to identify and prioritise how common vulnerabilities and threats across smart networks could potentially trigger a systemic crisis.

Assessment of Principle #3' Understanding cyber security governance and skills'

There is limited guidance within this principle on the following points:

- e) What elements within the operations need to be governed by the LA and how the cyber risk governance can be established for the connected place ecosystem in the LA's procurement life cycle (where multiple services are procured through multiple operators).
- f) what skills and capabilities need to be upgraded for efficient governance of the connected place ecosystem

The NCSC guidance provided a link to the organizational governance for security risks; however, it did not contain explicit guidance as required by the LAs to govern the cyber security and resilience risks of cross-sector smart services within connected places.

Assessment of Principle #4 'Understanding your suppliers'

This principle could be enhanced to include how the following can be assessed a) maturity level of the security operations, and b) risk that connected place ecosystem operations are exposed to suppliers with links to hostile countries.

Assessment of Principle #9 Designing your connected place to be resilient and scalable

The cyber risk indicators are not defined for the LA to obtain visibility of how cyber risk exposure of the smart services, and the connected ecosystem can be assessed.

Assessment of Principle #10 'Designing your connected place monitoring'

This principle does not specify a method that explains how relevant security events from the logs across the interconnected systems within the networks owned by various organizations can be joined up to interpret a threat.

Assessment of Principle #12 Managing your connected place's supply chain and Principle #13 Managing your connected place throughout its life cycle

There is a lack of an audit process and assurance framework for the connected place ecosystem. Guidance is also required for selecting appropriate and proportionate measures that form adequate security levels for reduction of the cyber risks.

Assessment of Principle #14 'Managing incidents and planning your response and recovery'

This principle can be enhanced to provide specific guidance to a) specify requirements in the procurement process to test the response plans and, b) manage recovery of the services in the event of a cyber-attack on a smart service which spreads to the connected place ecosystem. “Dry runs” against cyber-attack scenarios for end-to-end services could be a core part of the principle.

The gaps were discussed within the focus group, and it was recognised that it might not be clear as to who needs to provide the additional guidance.

5.4.2 Thematic analysis of gaps in the procurement process

The gaps in the procurement process of the LAs were analysed to identify, and subsequently (through the focus group) understand the key themes. The process followed for the thematic analysis is described below.

- i) All gaps were identified from the notes of each stakeholder interview.
- ii) The list of gaps was reviewed and as per the procurement process that included the tender, bids, contract award, contract management and service continuity as followed by the LAs (see Appendix 5-A).
- iii) Unique thematic gaps were identified, and gaps that appeared similar or associated with each other were combined (for example, the lack of specifications for operational monitoring and tests for resilience were combined under one gap), where appropriate.
- iv) The gaps under each theme were further analysed to separate the associated barriers, as well as challenges (see Appendix 5-B). It was validated that the themes were accurate representations and were present in the gaps.

The following five themes emerged and will be discussed in turn:

Theme 1: Lack of accountability for cyber risk management for the connected ecosystem

Theme 2: Insufficient and inconsistent cyber resilience specifications in the CPO contracts

Theme 3: Lack of Operational Governance by the LAs for cyber risks across smart services

Theme 4: Lack of Assurance by the LAs for cyber risks for smart services, as well as the ecosystem

Theme 5: Inadequate skilled resources and capabilities in the LAs

5.4.3 Root-Cause Analysis

A root-cause analysis was based on the “5-whys” methodology for the above themes and the findings were discussed with the focus group. The analysis was done by going through multiple causal factors mentioned by the stakeholders during the data gathering phases which were associated with the barriers and challenges identified during the thematic analysis. The strategy adopted was to identify the problems in each theme, by drilling down into each of the issues to understand “what caused the problem”. The cause identified was treated as an issue and was further analysed to understand what caused it. This was repeated up to three times until the researcher had moved past the symptoms and identified the potential actual root cause. Based on the discussions with the stakeholders and the notes from the interviews, the root cause was identified from three iterations instead of five iterations. This was discussed within the focus group, and it was agreed that three iterations were sufficient for this analysis based on the limitations of the gathered data.

For each of the themes (Figure 5-4 to Figure 5-8), the researcher discussed the root cause analysis and incorporated the feedback provided by the focus group. However, at this point it must be noted that the root cause analysis has its limitations. The analysis is based on the views of the participants in this study which is a small sample and hence may or may not reflect the issues across the LAs in the UK. The analysis based on ‘5 whys’ method oversimplifies the problem with a conclusion that there are one or more root causes for a problem to occur, which restricts the wider view of how multiple factors contribute to the unfolding of the problem (Card, 2017) . These limitations were discussed within the focus group and the results were summarised considering these limitations.

5.4.3.1 Theme 1: Lack of accountability for the cyber risk management of connected ecosystems

As seen in Figure 5-5, the focus group reached agreement that the root causes for this theme were potentially two-fold a) lack of Government guidelines on what is required to be accountable for the connected place ecosystem, and b) a mismatch in

expectations mentioned in the Government guidelines and understanding within the LA procurement function. As per Government guidelines (in the Manual for smart streets, as well as in the NCSC connected place guidelines), the connected place owner is the risk owner of the connected place ecosystem that they are building. However, the LAs seem to be unaware of the ownership of cyber risk management for the connected place ecosystem.

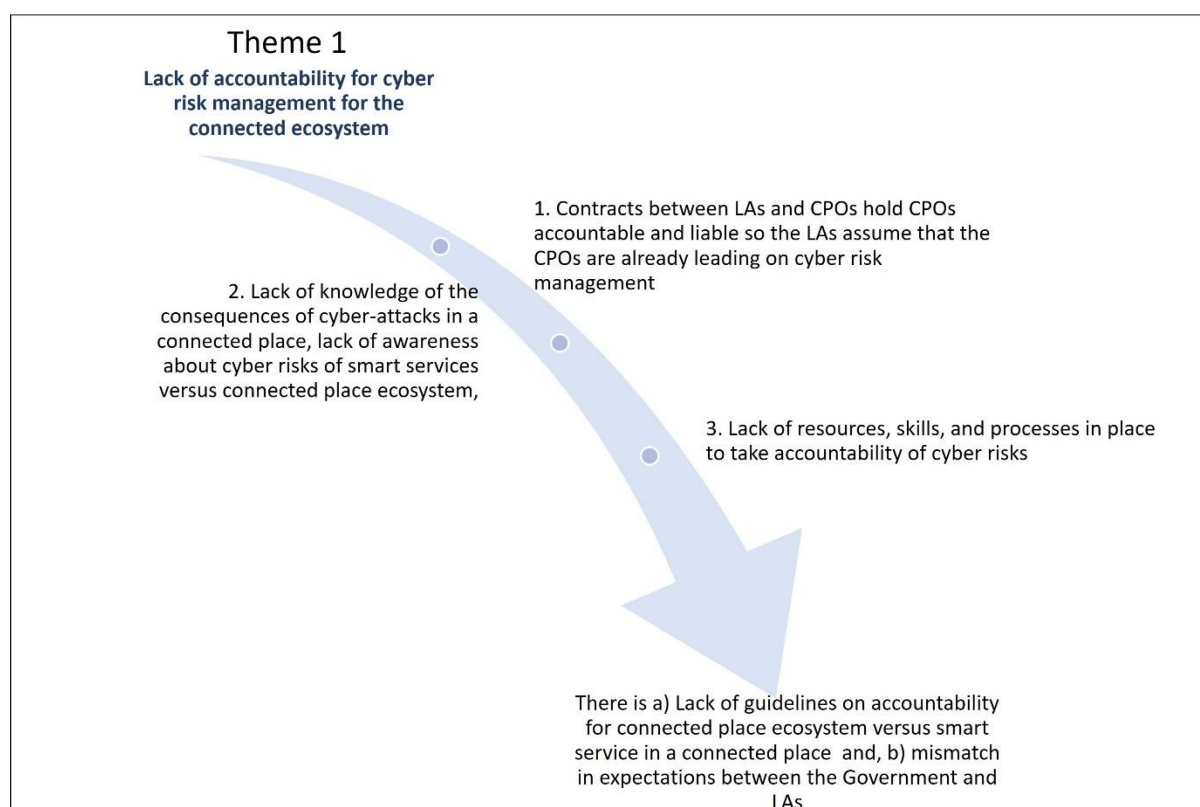


Figure 5-5 Theme 1 - Root cause Analysis

The LAs have traditionally followed a model for the procurement of services in which they are not liable for any incidents. For example, as discussed above, if they provide parking land on lease to a private operator, the LAs are not liable for a parked car being vandalised. This model may not work for digital services in a connected place as the cyber risks, if not managed, can impact CNI and essential services. Interim ownership needs to be in place to create accountability for the cyber risks in the connected place ecosystem until the LAs are ready to own and govern it.

5.4.3.2 Theme 2: Insufficient and inconsistent cyber resilience specifications in CPO contracts

As seen in Figure 5-6, the focus group collectively thought that the root cause for this theme was lack of mature consistent policy, guidelines, and standards that could have helped the LAs self-assess the requirements for cyber resilience of smart services as well as the connected place ecosystem within the procurement process. As discussed earlier, the draft Manual for Smart Streets offers 12 use cases with specific standards to procure services, including EV charging, which is expected to be rolled out in mid-2023. The cybersecurity guidance being developed in this manual is generic and designed for application across use cases, which could pose a challenge for LAs trying to apply it to the procurement process.

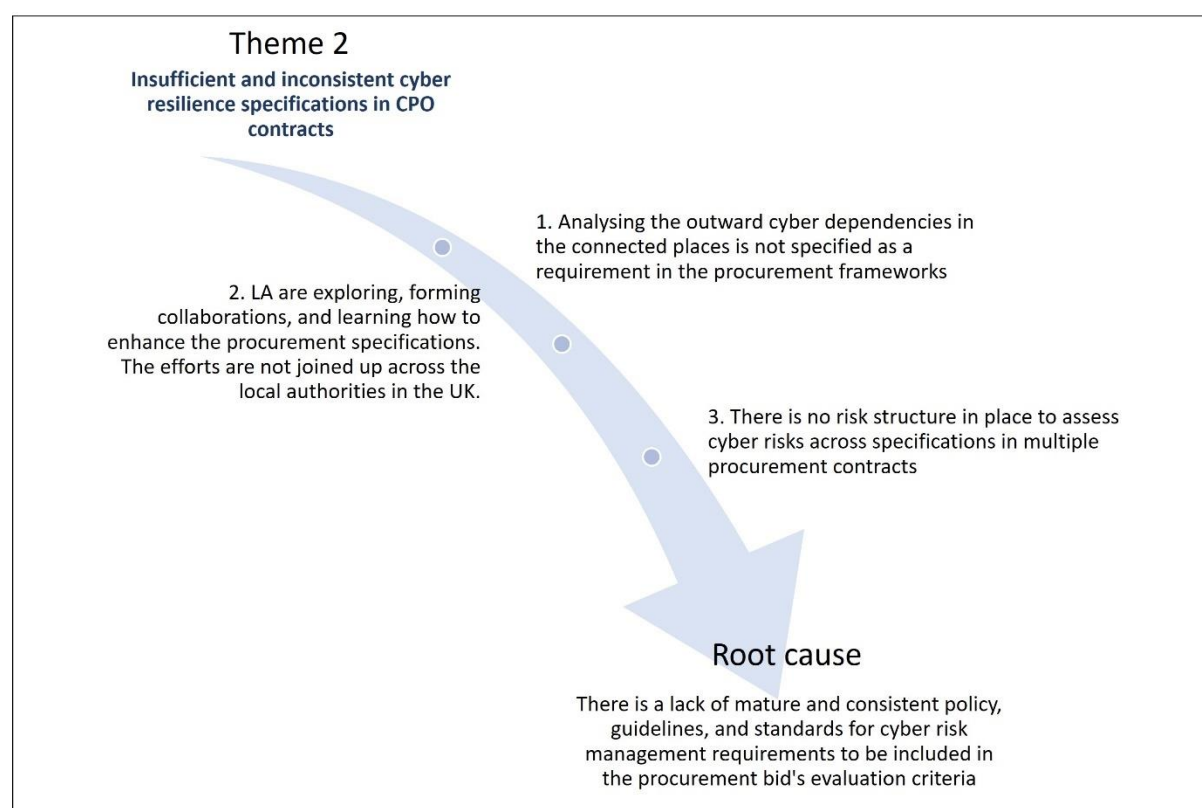


Figure 5-6 Theme 2 - Root cause Analysis

The lag in implementation / maturity of policy, standards and guidance results in processes not established with the right controls. Interim measures need to be provided to the LAs and the development / maturity of policy as well as guidance needs to be accelerated.

5.4.3.3 Theme 3: Lack of Operational Governance for cyber risks across smart services

As seen in Figure 5-7, the root cause for this theme, as per the agreement within the focus group was a lack of governance structure in place for the connected ecosystem. Additionally, there is inadequate guidance regarding reporting metrics, analysis of the monitoring of reports and the risk indicators that enable the LA to be setup for operational governance of the connected place ecosystem.

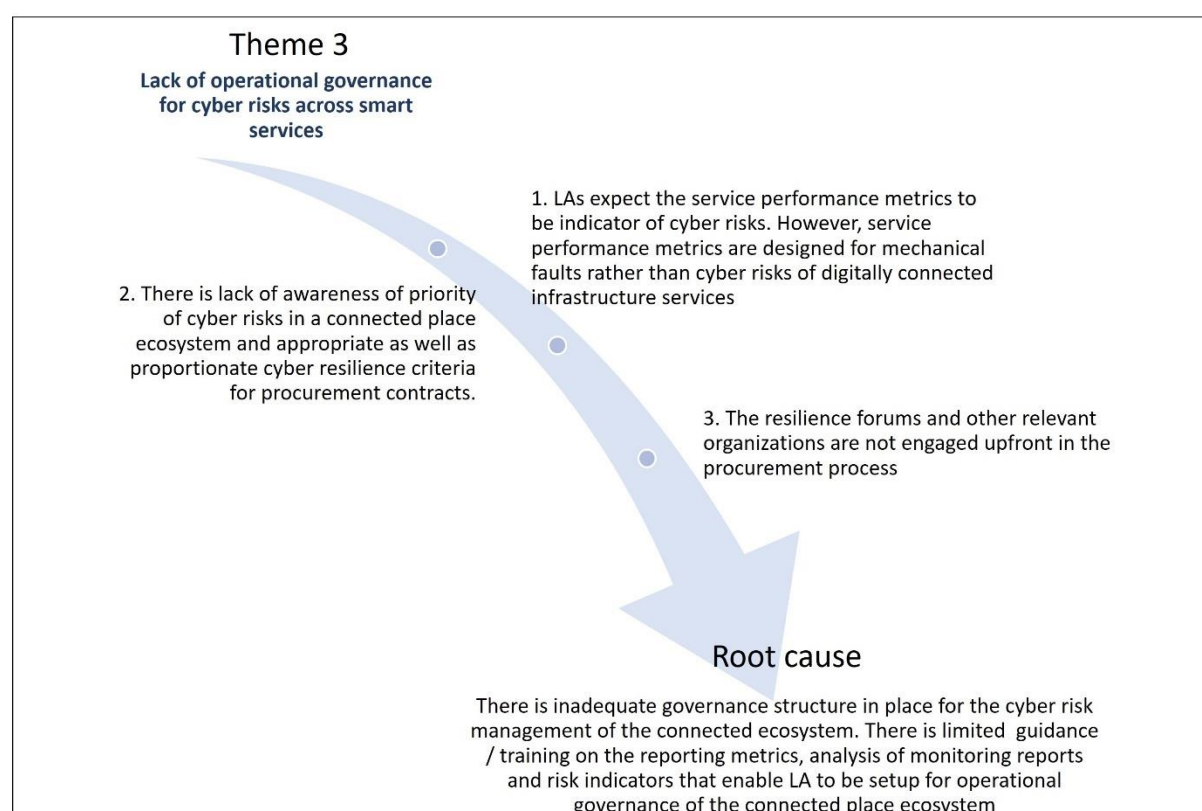


Figure 5-7 Theme 3 - Root cause Analysis

CPOs also need guidance for managing cyber risks from the viewpoint of potential cyber warfare threats, for example, a hostile nation affecting the CNI services in the ecosystem, through an attack on the EV charging service (see section 5.4.1, Assessment of Principle #4).

5.4.3.4 Theme 4: Lack of Assurance by LAs for cyber risks for smart services, as well as the ecosystem

As seen in Figure 5-8, the potential root cause for this theme proposed by the focus group was a lack of guidance for the governance mechanisms to assure the

operational cyber risks of smart services (not just IT focussed assessments) and the connected place ecosystem. There is no guideline available

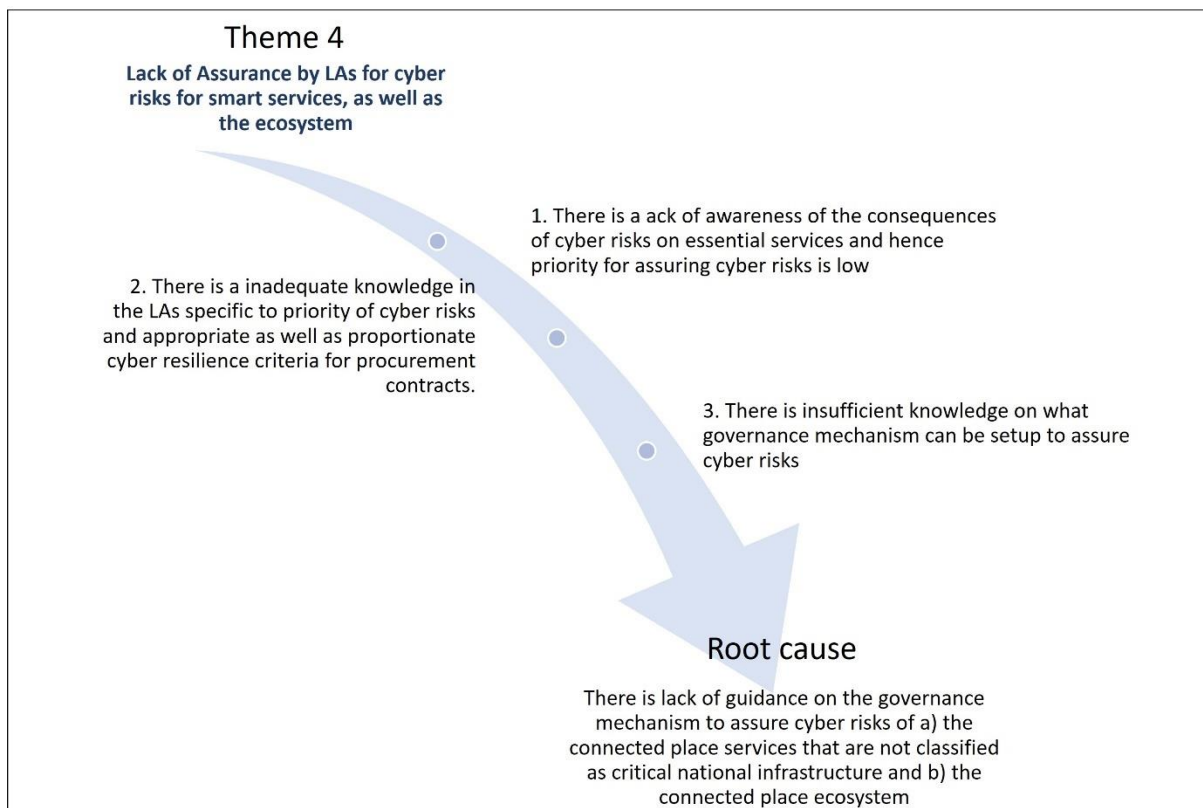


Figure 5-8 Theme 4 - Root cause Analysis

from the NCSC on the auditing and assurance of smart services, as well as the connected place ecosystem (as highlighted in Section 5.4.1 above).

5.4.3.5 Theme 5: Inadequate skilled resources and capabilities in the LAs

The Government guidelines expect the LAs to own the cyber risks of connected places, however the required capabilities, skills and resources are yet to be matured. As seen in Fig. 5.9, the focus group believed the root cause was the capability development lagging behind the rollouts of smart services. This is due to inadequate assessment of the requirement for enhanced capabilities and appropriate ownership structure to rollout the connected infrastructure services and manage the cyber risks of a connected place. The UK Government is already working on development of capabilities and skills to ensure a secure connected services in the street ecosystem (NCSC, 2022a).

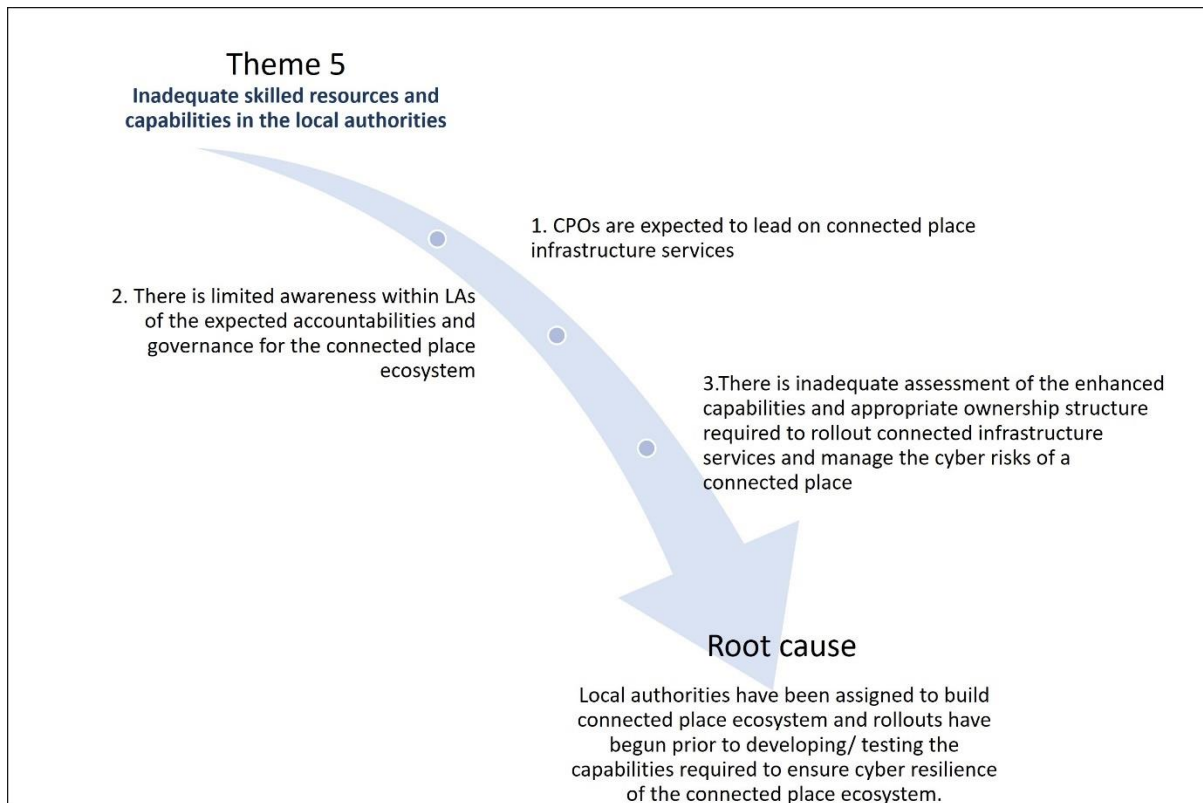


Figure 5-9 Theme 5 - Root cause Analysis

It was recognised that these root causes need to be reviewed by individual organizations such as local authority or Government departments to understand how to best place address them and which organization can take it forward. Section 5.5 provides recommended tactical and strategic ways to address the root causes for the thematic gaps in the procurement process and the gaps in the Government (includes NCSC) guidance.

5.5 Discussion

This study analysed the procurement process for smart services, NCSC guidance for cybersecurity of connected places and the challenges in managing the cyber resilience risk exposure to the CNI services. It was found that the LAs procuring smart EV charging service are aware of high-level potential cybersecurity requirements. However, they have not thought through the fact that the risk interfaces in the powerful EV chargers and potential security flaws combined may inadvertently create a vulnerability that threat actors could use to cause widespread power cuts and other major disruptions in a connected place ecosystem. The findings from the EV charging case study align with the EV energy Taskforce which notes that the Government and industry must ensure 'system resilience by design' to mitigate against both physical

and cyber system vulnerabilities relating to the digital integration of EVs and charging infrastructure (EV Energy Taskforce, 2023). This is particularly important because it is expected that by 2025, more than one quarter of all new vehicles being sold globally will be electric or hybrid; and these organizations typically bolt on cybersecurity as an afterthought, presenting further security and resilience risks (Fridman, 2023; Feller, 2022).

NCSC cybersecurity guidelines for connected places are intended to help the LAs to “build awareness and understanding of the security considerations needed to design, build, and manage their connected places” (NCSC, 2021b). The guidance is also intended to support security considerations for singular or multiple service functions in the connected public realm (NCSC, 2021b). This study, however, suggests that the guidance is fragmented, difficult to action and falls short of achieving this purpose. Although the LAs assure available security standards during procurement contract award and CPOs follow the IT standards for operational risk management, the measures for connected place security, as well as resilience by design in the procurement process lifecycle are inadequate.

The key findings for the current study are twofold:

- 1) There is a lack of governance and risk structure in place for the management of systemic cyber risks across multiple service functions within the connected place ecosystem, and
- 2) The cyber resilience requirements managed by the LAs in the procurement process fall short of addressing the probability of potential high-profile crime scenarios that could have cascading impacts across the connected place.

These findings are in sync with academic research which suggests that during the operationalisation of smart infrastructure, the risks resulting from technical, economic, social and environmental implications are not fully recognized (Vitunskaite et al., 2019; Wielicka-Gańczarczyk & Jonek-Kowalska, 2023). Research on Smart London projects have also suggested that the guidance for smart infrastructure rollouts is focused on the implementation of the smart projects while a) the detailed guidance on implementing the high-level security standards is inadequate and b) a governance model across smart projects for the security of connected places is yet to be embedded (Vitunskaite et al., 2019). Studies have additionally observed that across multiple local authorities with shared budgets/staff, fragmented inadequate governance has also been observed in public procurement process that involved

testing as well as implementing urban smart solutions iteratively (Coletta et al., 2019; Lopes, 2017).

The findings from this study are further analysed below through the lens of security as well as resilience risks for essential services especially for an evolving connected ecosystem, comprising a range of new as well as legacy infrastructure (expected to be smart) and thereby providing a larger attack surface. A set of recommendations are also provided for the NCSC Connected places team, policymakers, LAs, local resilience forums, police force, urban planners, smart service operators and the Government departments.

5.5.1 Capabilities for management of systemic cyber risks in the ecosystem

Smart EV charging depends on various software systems running on various hardware platforms from many vendors connected by multiple communication systems. This complexity creates the risk of conflicting controls, unforeseen behaviour and a high risk of cyber compromise in the ecosystem (Sygensys, 2022). The Critical Infrastructure Security Agency (CISA), the US federal reporting agency responsible for security disclosures has issued multiple alerts about smart EV charging stating that the individual components being cyber secure does not assure that systemic risks are managed (Gordon, 2022). As discussed initially in Chapter 4 systemic risk is the risk to be addressed urgently to contain the consequences of a cyber-attack spreading catastrophically across systems, networks, sectors, and geographies; far beyond the infrastructure/ component/device that has been attacked and possibly disrupting a critical national essential service (World Economic Forum, 2016; Zurich Insurance, 2018; Cunningham et al., 2018). The systemic problems could not just cause catastrophic harm but also “spread this harm with a unique combination of speed, scale and uncertainty” (ESRB, 2020). A cyber-attack through an attractive target such as an EV smart charging service that disrupts links between multiple non-critical entities, a systemically important service or a strategically important organization can trigger a ‘domino’ effect i.e. a systemic event across energy grids and national/global systems (Jones et al., 2020; Fridman, 2023).

Traditional cybersecurity approaches are limited in their ability to understand and deal with systemic risks due to their necessary focus on single entities, systems, and supply chains. However, the findings from this study indicate that the LAs continue to follow these traditional approaches for the procurement of individual smart services

from CPOs, with additional checks for the standards available for connected products and devices. As already discussed in Chapter 4, section 4.3, there needs to be a clear policy intervention and consistent framework for security of connected places that is owned by a lead Government department and sets the direction for procurement and operations of smart services. The policy interventions need to align with the national cyber security strategy 2022-2030 that aims to develop capabilities for centralised governance to identify and oversee systemic cyber-security risks across sectors (NCSC, 2022c). DSIT could include connected place capability metrics in their annual survey that assesses the national cybersecurity capabilities (DSIT, 2024a). This could help benchmark the capabilities and create appropriate roadmaps for capability enhancements.

The study found that there is a lack of risk structure, ongoing threat assessment and dependency analysis for the management of systemic risks across multiple services owned by multiple organizations in the connected place ecosystem. The LAs are assumed to be the owners for the purposes of ensuring security and resilience of connected places as seen in the Government approaches, as well as guidelines. However, they are not set up with the capabilities, risk policies, guidance, resources, governance structure, training, or the skills to do this. Clear accountabilities, governance and assurance need to be defined and implemented to assure the cyber resilience specifications in contracts for smart services are adequate. DSIT's governance in a box approach (DSIT, 2024b) provides generic process guidelines, but falls short of guidance for governance of systemic security risks and events. Understanding the level of systemic cybersecurity risk exposure in connected places and managing it is challenging as this is an area that is yet to mature while the technology and innovations advance in a fast-paced manner (Johnson, Berg, et al., 2022).

The initiative within the TTF to provide start-up documentation for people, processes, roles, and responsibilities points to the fact that there is a keen interest in working towards the goal of operationalising efficient as well as secure services that meet the needs of citizens in connected places. The LAs and CPOs are keen to collaborate and engage with initiatives that help enhance the security of smart services. There are multiple initiatives run by the Government to support the LAs which are noteworthy, such as the Manual for smart streets that maps standards per use case (Transport Technology Forum, 2022), BSI PAS 185:2017 standards (CPNI,

2022) for holistic security, the potential policy for connected places (DCMS, 2022a), security framework for devices interfacing with the energy grid (EV Energy Taskforce Working Group 3, 2021), regulatory controls for smart metering system devices that enable EVs (Department for Business Energy & Industrial Strategy, 2021), smart EV charging regulations (Legislation.gov.uk, 2021), and the UK Government's consolidated playbook that support LAs in governance as well as risk management of connected places (DSIT, 2023). Additionally, the vendors from countries deemed politically hostile, are now also subject to restrictions in the UK (Dowden, 2022). However, these standards, guidelines and policies are lagging behind considering that by 2025, the government aims to ensure that all EV charging stations are smart (OfGem, 2023). They also do not provide a methodology for monitoring, managing as well as assuring systemic risks across multiple services owned by different organizations within a connected place ecosystem.

Monitoring the systems and alerting when an anomaly occurs is a part of traditional IT operations and is implemented by the CPO. The approach to cyber security follows the original concept of monitoring individual servers, data protection, disaster recovery and business continuity for IT systems as well as services owned by each organization. However, within a connected place, the security risk monitoring involves joining up anomalies across multiple networks owned by different organizations and analysing changes to the threat landscapes to understand its significance for the security of the whole ecosystem. This is extremely complex and guidance within the NCSC cybersecurity principles for connected places does not provide insights into this complexity for detecting and getting early warnings of cyber threats within a connected place ecosystem. Considering the inter-connectivity of smart infrastructure, it is critical to understand how the recovery governance will work in the event of a cyber-attack across multiple service providers. There is lack of clarity around recovery plan for disruption in a connected place across multiple service providers (such as ransomware spreading beyond the city's CPO networks).

City authorities and resilience forums do understand that the environment is changing along with the threat landscape, and that they need to adapt to it. City resilience forums need to upscale their efforts for the assessment of response and recovery preparedness in the event of a large-scale systemic cyber event in a connected place. Government needs to define the roles, capacities, accountabilities, and capabilities across stakeholder communities (including police and resilience

forums) required to establish systemic risk authorities that can govern and assure the systemic cyber risks of smart ecosystems wherein smart services are being rolled out. Cyber resilience testing by running simulated attacks across critical elements of the networks and services need to be conducted prior to a major rollout so that city authorities do not just accept new technology that could be a security threat (Epiphaniou et al., 2023; S, 2019; Salvi et al., 2022; Whitmore, 2020). Practicing response plans to operational cyber risks on a regular basis is also recommended by NCSC (NCSC, 2022a).

The Government has provided NCSC Capability Assessment Framework (CAF) as a security audit and assurance framework to manage cyber risks. It could be enhanced and used for assurance of cyber risks in connected places by LAs and suppliers (DSIT, 2024b). In the interim, the NCSC Connected place guidelines and the DfT initiatives such as TTF as well as the Manual for smart streets could include guidance to establish systemic risk management organization aligned to the procurement process used to procure smart services. The NCSC connected place guidance could be extended to include cyber risk metrics and tools to address concentrated sources of cyber risk. The approach recommended by the Cyber and Security Infrastructure Security Agency (CISA), U.S. Department of Homeland Security (CISA, 2021) can be customised for this purpose. References can also be made to NIST SP 800-160 guidance for systemic resiliency (Ross et al., 2015). Mitigating systemic risk through a scenario based simulation is a very strong strategic as well as tactical approach to managing risks in a connected place ecosystem (Zukis, 2021). To help urban designers to build security into their designs, an expert team could develop a tool to simulate a model that has two layers of connectivity – physical and virtual to understand the concentration of contagion risks in the ecosystem (Goh et al., 2020). There needs to be complete visibility of the how the street environment is connected (including inter-related and inter-dependent systems and services). Further, there needs to be an awareness of the resulting threat landscape, common vulnerabilities, potential cascading impacts of cyber-attacks, levels of security risks and security measures to counter these risks.

The LAs have been assigned to build the connected place ecosystem and rollouts began prior to developing/ testing the capabilities required to ensure cyber resilience of the connected place ecosystem. There needs to be a full assessment of whether local authorities are the right organizations to own and govern connected

place security. A clear governance policy needs to be drafted that addresses what changes are required within the business processes and capabilities required to roll out smart infrastructure to build a connected place ecosystem that is resilient by design, keeping in mind that threat actors could be a nation practicing cyberwarfare. The NCSC could roll out training and upskilling courses for resilience forums to be more proactive in terms of preparedness in the event of cyber-attacks. Programs need to be initiated for the development of relevant skills to support the personnel responsible for transforming the street scape. There needs to be a prioritised overall joined up effort within Government departments, the public sector, academia, and private companies to work out a systemic risk management approach to reduce exposure to the multiplying cybersecurity threats within connected places.

5.5.2 Management of cyber resilience in the procurement process of smart services

Although the LAs feel responsible for the rollout of smart infrastructure, there is a gap in awareness of the cybercrime impacts for connected places. This is in direct conflict with Section 17 of The Crime and Disorder Act 1998 (CDA) which stipulates that LAs are required to “consider the crime and disorder implications of all their activities and functions and do all that they reasonably can to reduce these problems” (UK Government Legislation, 1998). There needs to be a unified view of the potential cyber risks in connected places to ensure the right prioritisation for the management of cyber risk exposure within the procurement frameworks and the LA’s procurement processes. The city authorities implementing smart solutions work collaboratively with the private sector and it is extremely important that the collaborative governance of the connected place ecosystem is implemented and ensures that the transformation of public services do not create any black boxes (Almeida et al., 2018; Lim et al., 2023).

As explained by the NCSC Connected place guidelines, understanding the level of cybersecurity risk exposure in connected places is challenging because this depends on multiple smart infrastructure, data stores, and connectivity to other smart services amongst many other factors (Johnson, Berg, et al., 2022). There is not enough clarity on security and resilience risks for common dependencies across networks such as public wifi within a connected place in the guidance. To prevent EV charging services from becoming a systemic risk to vehicles and the energy grid,

cyber threat intelligence could be regularly provided by the NCSC (or any other relevant organization identified by the Government) to the LAs and the CPOs (ESRB, 2020). The LAs need to be working with private operators to conduct specific scenario based potential crime threat assessments in connected places to crystalise the security as well as resilience needs. Development of cyber incident simulation scenario models (Ficco et al., 2017; Heidari et al., 2023; Kavak et al., 2016; Nicol, 2005) emerging from a smart infrastructure affecting connected places adversely using technologies such as digital twins will help inform the approach (Epiphaniou et al., 2023; Heidari et al., 2023; Jones et al., 2020; Salvi et al., 2022). Perhaps similar threat scenarios (including insider threats such as a supplier taken over by a company affiliated with a hostile country) could be developed and introduced into the NCSC guidance or the DfT Manual for Smart Streets or alternate initiatives to support the stakeholder community. Guidance needs to be provided for specifications to be included in the procurement contracts to balance between limiting the risk exposure of a cyber-attack and providing appropriate and proportionate measures for cyber risk management. The procurement frameworks need to be analysed and with NCSC guidance could mature further to include more structured deterrence, response, and recovery methods for the governance of the cyber risks in the connected place ecosystem. EV infrastructure service specifications across the LAs and the supply chain for all components involved (such as end points, vehicles, applications for customers, payment systems, cloud provision, front office, and back office) need to be synchronised for stringent security (Mookerjee, 2022). UK Government has already proposed to provide outcome-based security requirements based on BSI standards, security testing and an assurance framework that meets the proposed regulatory requirements for EV charging (Department for Transport, 2019a). The NCSC cybersecurity principles for connected places could additionally provide the necessary training for the LAs to identify and prioritise cyber risk management in the procurement process. This will enable the LAs to reduce the risk of the loss of trust or reputational damage in event of the cyber-attack. It can also change the position of power for the LAs with skills to assess the CPO services. It will also resolve the gap in the Government guidelines where the LA are expected to own and govern the cyber risks of the smart services being procured.

The UK Government's reforms for the public procurement process could include the procurement of smart services within the connected places. For example

Innovation in procurement for London's authorities (LOTI, 2021), the Procurement guidance (Local Government Association, 2019) and Regulations 2024 (Legislation.gov.uk, 2024) could be joined up to help embed security-by-design in smart service procurement within UK's connected places.

The general feedback from the LAs for the NCSC guidelines is that they are usually at a very abstract level and are difficult to translate into concrete actions due to lack of experts in the industry (Shukla, 2021). The LAs reported that they find it tough to navigate the plethora of guidelines from various sources and it is not the function of the procurement team to absorb such wide-ranging guidelines to make the cyber risk management decisions. NPSA has commissioned BSI PAS 185:2017 standards specific to a security minded approach while building connected places (CPNI, 2022) which also explains how to conduct a city-specific security risk assessment. However, the LAs need expertise to translate these into action. Absent clear standards and regulations, the LA professionals need more support from Government for a customised set of consistent cyber resilience mitigation specifications to be included in the procurement bid.

The gap analysis provided evidence that the LAs and CPOs complied with regulatory requirements stipulated within the NCSC cybersecurity principles for connected places. In the UK, the Network and Information Systems (NIS) legislation mandates cyber risk management for CNI (DCMS, 2023). However, although EV charging connects two essential services – transport and energy, it is not yet defined as CNI. With approximately 28 thousand public electric vehicle charging devices in the UK in Jan 2022 (Department for Transport, 2022), the UK public charging network has potentially doubled by the end of 2023 (O'Sullivan-Dale, 2022) and increase to 300,000 by 2030 (Transport and Environment, 2022). As such, the EV charging infrastructure could be declared as CNI soon. Research has evidenced that NIS regulation was limited in terms of managing the cyber security risks of cross sector services (Shukla et al., 2019). This was also echoed by a few stakeholders in the interviews conducted here. EU countries have extended the NIS legislation (that mandates cyber risk assessment) termed as NIS 2.0 to include multiple other sectors such as smart infrastructure. Brexit has resulted in the UK not being obliged to implement the NIS 2.0 Directive and hence there is currently no regulatory mandate to manage cyber risks of the smart infrastructure. The UK Government has proposed improvements in cyber resilience by focussing on managed services of the supply-

chain and strengthening cyber risk management for sectors already covered by NIS legislation (Clark James & Cook David, 2022). This aspect of managing cyber risks within connected places could be covered in the improved measures for NIS legislation. In readiness for the same, the LAs and procurement frameworks could ask for cyber risk audit reports in the procurement process using guidance from the NCSC Capability Assessment Framework (CAF) (NCSC, 2022b). This will also resolve the issue of skilled resources required to use the NCSC cybersecurity principles for connected places to manage cyber risks as they are not a part of standards, procurement framework or any mandate from the Government.

Place-based urban designs play a crucial role not just towards building e-governance for both physical and virtual place management of a community, it also provides insights to help develop crime prevention policies in micro places (Ashby, 2019; Walters, 2011). According to the Routine Activities Theory (RAT) in crime science, crime occurs when a motivated offender meets a suitable target (person or object) where there is an absence of three types of crime controllers - intimate handlers, guardians, and place managers (Cohen & Felson, 1979; Sampson et al., 2010). The spatial and temporal crime concentration patterns based on the convergence of offenders, targets and controllers in space and time has allowed evolution of various place-based strategic interventions. In a physical space, the crime hot-spots could be a dark alley on a corner of a street whereas in virtual space, the crime hot spot could point to selected virtual IPs resulting from insecure networks connecting through public wifi (Hsieh & Wang, 2018). In the on-line space, the controllers (such as information security officers) implement controls for place management (such as security awareness programmes) to improve the resilience of organizational services (Back & Guerette, 2021). RAT also suggest that the effectiveness of the controllers is potentially linked to their relationship with super controllers (such as regulatory authority) who can persuade the controllers to be more effective in preventing crime (Sampson et al., 2010). The protection from any cybercrime is as strong as its weakest link (Hsieh & Wang, 2018). While there is limited research on effectiveness of place management interventions for cyber space (Back & Guerette, 2021), there is an additional challenge of the need for adaptations as well as better cyber risk governance with changing on-line environments, advance of technology and further threats from the fact that hackers keep evolving their methods (Riley, 2021).

Expert teams in the Government could initiate pilot risk analysis projects and establish continuous assurance mechanisms for procurement frameworks and processes for smart services rather than leaving it to the individual LAs. LOTI plays an important role as a controller to support the LAs in London in improving the public services with the advent of smart technologies (LOTI, 2020b). A similar organization could be setup as a super controller to bring consistency, develop capabilities and support the LAs across the UK. This would also allow continuous and consistent assessment of the interdependencies between new technologies and innovations across sectors working together with the smart infrastructure in connected places. There needs to be potentially a structural transformation in the organizations such as the LAs or a separate organization needs to take the responsibility for reviewing the combined impacts across procurement contracts within a connected place ecosystem. As summarised by Theo Blackwell (the LA and Digital head of London), for the procurement model to be successful there needs to be transformation of the operating model for the LAs all over the UK, specific to “governance, roles, risk management, decision making, policies, democratic process, citizen engagement, staff responsibility, structures and, of course, processes” (Local Government Association, 2017). There needs to be a regular assessment of whether security interventions address the changing criminal landscape and what are the costs versus the benefits. A knowledge base of “what works” for connected place security and resilience needs to be developed.

5.6 Conclusion

The aim of this study was to explore whether the procurement process followed by the LAs in the UK for smart services was robust enough to enable the LAs to reduce the systemic cyber resilience risks to connected CNI services (such as energy and transport) in the connected place ecosystem. The findings suggest that the Government, LAs and the CPOs were working collaboratively, however, cyber resilience risks to connected CNI services may not be systematically identified, owned, and governed within connected places. The criminogenic effects of smart street elements on the connected ecosystem need to be monitored due to the continuous transformations brought by fast-paced changes to technology and the innovation cycle. The UK government and industry are lagging in the development of measures to prevent as well as be prepared for the magnitude of systemic cyber risks in

connected places. The findings from this study could facilitate a deep dive into the quality of measures used to build resilience against crime, how to address the challenges faced and to analyse whether guidelines within the NCSC cybersecurity principles for connected Places were fit for purpose.

There has not been sufficient research on crime and place in context of connected places. The key limitation of this study was the willingness of stakeholders to participate in this research and potential reluctance to provide in-depth responses which could point to the short comings of the organizations that they work for. Hence, the study is based on the limited view of the small sample of stakeholders who participated and provided agreement for their views to be published. The findings are specific to the EV charging case study and although the generic procurement, operations and cyber risk management are potentially applicable to the other smart services, there is no definitive evidence for this. This study was conducted for only one use case with only seven participants from the LA and only one CPO. The findings, hence, may not generalise to other areas and organisations in the UK. Another key limitation is that this study is a snapshot in time (March 2022- March 2023) and hence may exclude developments that have happened after the data was collected. The data was gathered over a period of a year and hence the results of the study were shared with the focus group as well as all stakeholders to assure its validity.

Recommendations were provided to assure that the connected ecosystem is resilient by design against potential crime and incorporate policies for systemic cyber risk governance within the procurement contracts for smart services in the ecosystem.

Chapter Six

6. Summary and Impact of this research

The aim of this research was to answer the research question “How might changes to urban elements in the street environment affect physical and cybercrime risks?”. The ongoing transformation of the built environment is currently being driven by the integration of technology and innovation, creating not just connected places (previously known as “smart cities”) but also new crime opportunities. This research addresses a gap in the literature by examining the impact of evolving crimes and security interventions in the street ecosystem shaped by the integration of physical and digital elements creating connected places.

Initially, the research introduces theories of environment criminology and the criminogenic features of urban street elements that influence crime patterns. A narrative review was then conducted to understand how digital urban elements are shaping the connected places, and how the application of principles of environment criminology might help to understand and address physical and cybercrime at connected places.

6.1 Research stages and findings

The research was divided into three stages (as explained in section 1.3). In the first stage, to arrive at the current state of art, the research reported here takes stock of the existing literature to explore the distribution of physical crime patterns associated with (traditional) urban elements in the built environment. In second stage, the digital capabilities of the changing urban environments and resulting risks of cybercrimes as well as cyber-physical crimes of the connected street infrastructure and particularly their cascading impacts in the street environment were studied. In the third stage, the practices followed by UK Local Authorities (LAs) to manage the systemic cybersecurity risks of connected places in the roll out of smart street infrastructure were assessed to understand the challenges involved.

6.1.1 Stage 1: Criminogenic effects of urban elements of street environment

As discussed, the first research question to be addressed was – “Which urban elements have been quantitatively analyzed for their influence on physical crime using

micro spatial units, and what is their estimated overall effect on crime?”. To answer this question, a systematic review was conducted, for which data from studies that quantitatively analysed strengths of associations between urban elements and crimes using micro spatial units were collated. Where data allowed, a meta-analysis was conducted to estimate the size of the effect of each urban element considered on crime.

29 studies were identified that quantified the effect of urban elements on physical crimes using analyses conducted for microspatial units. Meta-analyses were conducted for eight urban elements, using data that could be combined and synthesized in a meaningful way. While many more studies exist, most had to be excluded either because they did not conduct analyses using data for micro-spatial units or because the statistical models used did not give comparable results. The eight urban elements for which data could be analysed were - street network configuration (measured in terms of accessibility and traffic flows), public transit stops, parks, schools, alcohol outlets, retail land use, drug treatment centers and bank branches & ATMs. The results of the meta-analysis indicated that all 8 urban elements were associated positively with crime in line with expectations from theories of environment criminology. The largest effects identified were for the association between main roads and public transit on violent crimes. This was followed by the effect of association between street configuration using betweenness as predictor and property crimes. The findings were in sync with past studies which suggested that more accessible and connected places which had higher pedestrian as well as traffic flows provided more opportunities for crime. To summarise, it was found that despite differences in studies, urban elements in the built environment shape the spatial and temporal distribution of urban crime in a consistent manner. While the findings from this chapter need to be treated with caution, due to the low number of data points and studies included for some of the analyses, they highlight how the design of urban environments can influence patterns of crime. While no studies were identified that examined in micro places - correlation of physical crimes with modern urban elements such as digital kiosks or cyber activities of people associated with urban elements, this research provided the direction for further research.

6.1.2 Stage 2: Digital capabilities and cybercrime risks of smart infrastructure

Moving from traditional feature of urban environments, the second stage of the research focussed on an analysis of the criminogenic properties of digitally connected urban street elements. This part of the study was divided into two sub-phases. First, the transformation of urban elements and the changing physical, cyber and cyber-physical security risks in the built environment were studied. A narrative literature review was conducted to explore the digital capabilities of smart streets, with a focus on four types of smart infrastructure (CCTV, lighting columns, EV charging and bus stops), and the cybersecurity challenges associated with them. Second, a study was conducted which focussed on an under researched area – the criminogenic effects of the digitally enabled street infrastructure and their collective systemic risks across the street environment in connected places. A systematic literature review was conducted to study how cyber-attacks on smart infrastructure could spread beyond the original system/network that is attacked (i.e. ‘cascading’ impacts) and result in a chain of security events (systemic events) in the built environment which could also affect the Critical National Infrastructure (CNI). The research question was: “In the event of a cyber-attack on smart infrastructure, what are the potential cascading impacts in the urban street environment?”.

The systematic literature review identified 16 cyber-attack scenarios with unique cascading impacts³ from 51 studies across three out of four use cases that were explored. Threat scenarios leading to first order cascading impacts (cascading failures in the network of the system that is subject to a cyber-attack) were found for two use cases – smart CCTV and smart lighting columns. Threat scenarios with first order, second order (cascading failures to the systems dependent on the network that is subject to first order impacts) and tertiary cascading impacts¹ (cascading failures to the systems dependent on the network that is subject to second order impacts) that could disrupt CNI were found for one use case - smart EV charging - which included impacts on the power grid, battery management systems of EVs, and service operators of EV charging stations. The literature reviewed did not provide sufficient information on the cascading impacts of threats beyond the immediate interfacing systems, nor did it provide information on the effectiveness of security interventions.

³ Cascading impacts of cyber-attacks – including first order, second order and tertiary order cascading impacts are explained in Chapter 4, Section 4.3

While the results discussed here cannot be generalized beyond the use cases examined, there were two findings. First, although only two real-life incidents of smart EV charging impacting CNI have been reported so far, the potential systemic security and resilience risks in connected places need to be addressed to protect the CNI. The transformation of connected places is still in its early stages, and there is a substantial risk of cyber-physical threats that need to be addressed proactively. However, analysis of security interventions in the UK suggested that existing standards, frameworks and guidelines do not refer to any overarching policy owned by a UK Government Department to manage the security and resilience of connected places. Academic literature pointed to the fact that cybersecurity, resilience, response, and recovery efforts currently focus on the individual organizational assets, interfaces, networks, and services of individual elements. There was no policy intervention designed for connected places. It was concluded that the provision of detailed descriptions of threat scenarios with cascading impacts that could manifest, could help establish security mechanisms with stronger accountabilities that anticipate and manage the cascading cyber risks involved in the design and operations of smart infrastructure services within connected places. The study has implications beyond the UK, but directly informs the UK Government, city authorities and urban planners on the gaps in embedding security and resilience in the designs and “anticipatory” policies of the changing street environment.

6.1.3 Stage 3: Cybersecurity risks of connected places

To review how the risks of cascading impacts discussed in the systematic literature review (stage 2) are managed, the challenges faced by the UK’s city authorities to minimize these risks and protect CNI were studied. The overarching purpose of this part of research was to address a gap in the knowledge base that would enable the Government, urban planners and city authorities to assess potential crime and security opportunities right from the design stage of traditional and smart urban street elements, and to inform the development of “anticipatory” policy that might address them. To achieve this, a study was conducted to explore how the UK’s LAs as connected place managers proactively managed security and resilience risk mitigation measures within the procurement process for smart infrastructure projects implemented by private operators.

Research has identified the need for more studies to assess the effectiveness of place management interventions to manage cyber risks (Back & Guerette, 2021), and the challenges faced by place managers as well as super controllers to adapt to the cybersecurity threats posed by technological innovations (Riley, 2021). This study was designed not only to address these gaps but also to raise awareness of the challenges LAs face as place managers in fostering a culture of preparedness and response to the growing cyber threats targeting CNI. However, their effectiveness as per environment criminology is linked to their relationship with super controllers (Sampson et al., 2010). Two UK Government departments - National Cyber Security Centre (NCSC) and Department for Science, Innovation and Technology (DSIT) were identified as the key super controllers responsible for supporting LAs in managing cyber risks of connected places. The NCSC is the national authority for cybersecurity guidance, while DSIT is responsible for ensuring that connected places are "secure by design," a key principle of Crime Prevention Through Environmental Design (CPTED). Therefore, initial discussions were held with DSIT, NCSC, and a selection of LAs at the outset of this research.

Two research questions were formulated: a) Do the procurement contracts for smart services specify measures for cybersecurity and resilience in line with the NCSC cybersecurity principles for connected places? and, b) Are there any challenges in managing the cyber resilience of the connected places? Smart EV charging was selected from the four use cases in stage 2, due to its potential to impact two CNI sectors: energy and transport. Research participants and stakeholders were selected from a range of organizations, including six LAs, Transport for London a private-sector EV charging service provider and three UK government departments - Department for Transport (DfT), DSIT, and the NCSC. A focus group was conducted with stakeholders who were experts in UK's connected place policies, connected place security and the procurement of smart EV charging services. Semi-structured interviews were conducted with the research participants, using a detailed questionnaire to assess a) their awareness of cascading impacts of cyber-attacks on smart EV charging which were explored in the systematic literature review in Chapter 5 and, b) if and how the NCSC cybersecurity principles for connected places are embedded in the procurement specifications and contract management process they use. The data collected from the semi-structured interviews was analysed to identify if there were gaps in the NCSC cybersecurity principles for connected places, and five

key themes were identified. A root-cause analysis based on the “5-whys” technique was subsequently used to investigate the underlying causes of the problems identified in each theme. Regular meetings were held with the focus group members to tap into their knowledge, get expert insights into the data collected and review the gap analysis.

There were four findings in this part of the study. First, this study reaffirmed the lack of clear national policy intervention regarding the security of connected places (a finding identified in stage 2). While the DSIT’s approach to the security of connected places and the NCSC’s cybersecurity principles clearly stated that LAs as place managers, were responsible for overseeing and assuring the cybersecurity risks of connected places, the reality was different. In practice, LAs lacked the necessary capabilities and were unaware of their accountability for managing the systemic risks associated with smart infrastructure services. This **disconnect** between national policy and local implementation of smart infrastructure governance highlights a significant gap in engagement between place managers and super controllers. Additionally, LAs also lacked the ability to translate fragmented cybersecurity guidance and standards into procurement specifications, thus placing private smart service operators in a position of power. As a result, although the procurement contracts for smart services specified measures for cybersecurity and resilience, there was no assurance check as to whether they were adequate to mitigate risks to cyber resilience or whether they conform with the NCSC cybersecurity principles for connected places. The governance and assurance of cybersecurity risks in procurement contracts were confined to private operators, who managed operational cyber risks in isolation for their services. This restricted the leadership role of place managers (LAs) in managing and monitoring the cybersecurity posture of connected places, particularly in relation to cascading risks to CNI.

Second, there was a lack of resilience (response and recovery) tests to understand the common connected threats, risks of systemic events and potential cascading impacts of cyber-attacks on smart infrastructure in the connected place ecosystem. Third, gaps were found in NCSC **cybersecurity** principles for connected places. There were inadequate standards, policies, and guidelines for LAs to create specifications in procurement contracts for the management of cyber resilience risks. Fourth, although the UK Government supports the LAs in implementing cybersecurity measures for smart infrastructure services, there was a lack of awareness within LAs

about potential criminal misuse, cascading impacts, systemic risks and unintended consequences of cyber-attacks on smart street infrastructure to connected places. As a result, it was unclear whether the cyber resilience mitigations in the procurement contracts for smart services were proportionate to the risks. The city authorities did not regularly analyse or monitor the criminogenic effects of smart street elements on their local connected ecosystems, despite continuous technological transformations.

6.2 Recommendations

The findings of stage 1 of this research aligned with the available research on crime and place which suggests that crime is concentrated at micro places and variations in crime patterns emerge when crime is analysed using micro spatial units. It is recommended that further research be conducted to analyse the effects of urban elements—both traditional, such as street configurations, and modern, such as digital kiosks—at micro-level places, as well as the impact of cyber activities on physical crimes.

Stage 2 and stage 3 of this research focussed on the prevention of crime for larger urban places connected digitally. It is important to analyse systemic crime events in connected places to enable full assessment of the crime concentration, variations in patterns and requirements for place management. The role of place managers is important for crime prevention in connected places. The place managers act as crime controllers by controlling crime or reducing criminal activities not just within physical spaces, but also in digital spaces (Eck, 2010). For instance, place managers are tasked with implementing and overseeing processes like maintaining strong cybersecurity protocols to prevent cybercrime, managing and reporting cyber risks to the board of directors, organizing educational programs to raise awareness about cyber threats, ensuring compliance with cybersecurity regulations, and conducting penetration tests, where ethical hackers simulate potential hacker tactics to assess the security of the virtual environment. Super controllers support the controllers and control their conduct (Sampson et al., 2010). In context of this research, key recommendations were provided for the LAs and associated stakeholders (acting as place managers) and the Government departments (acting as super controllers) to collaboratively enhance security interventions (such as providing clear guidance, policy, threat assessment, risk structure, training, awareness programmes, and capabilities) and promote governance, accountability as well as

assurance of connected places. Research on crime and place has suggested that crime prevention efforts are more effective when prioritized for high-crime places (Eck & Guerette, 2012). CNI is arguably one of the most attractive forms of target for a cyber-attack in connected places, and hence, the recommendations need to be prioritized to reduce the impacts to CNI (Eck, Clarke, & Guerette, 2007). It is extremely important to ensure that places have accountable owners that apply interventions that effectively alter the physical and virtual places in a way that influences peoples' behaviour positively to prevent a crime event (Eck & Guerette, 2012). Therefore, the key recommendations emphasize empowering LAs (place managers) to govern and ensure the security of connected places, while also continuously evaluating the effectiveness of place managers in maintaining security and resilience of connected places. More thinking could go into frameworks of place management in cyber and cyber-physical spaces.

The recommendations of this study are summarised below:

- i. **Continuous systemic threat assessments:** The continuously changing physical and digital built environment affects the crime and security landscape. Hence, on a continuous basis, there needs to be complete visibility of the how the street environment is physically and digitally connected (including inter-related and inter-dependent systems and services) and how this changes interactions between the built environment and people. Further, there needs to be an awareness of the resulting changing behaviours, threat landscape, common vulnerabilities, levels of collective physical and digital security risks in a place and security measures to counter these risks.

Crime scenario-based risk analysis of systemic events and cascading impacts of cyber-attacks across infrastructure services in the street environment need to be defined. For example, a) the Government of Ireland has published a map of dependencies across CNI to assess how cyber risks could result in systemic risks that affect the CNI (National Cyber Security Centre - Government of Ireland, 2022), and b) the Cybersecurity and Infrastructure Security Agency (CISA), USA, has provided guidance for the reduction of systemic risks (CISA, 2021). In the UK, the NCSC could support LAs by providing generic scenario-based simulations for systemic events in their quarterly threat assessments. A lead UK Government department should lead on conducting ongoing resilience (response and recovery) tests across connected places. There needs to be a regular assessment of whether

security interventions address the changing criminal landscape and what are the costs versus the benefits. A knowledge base of “what works” for connected place security and resilience needs to be developed.

- ii. **Holistic guidance:** The fragmented or insufficient guidance for security measures needs to be consolidated to enable holistic implementation to counter the physical and digital criminogenic properties of urban elements connected in the street environment. Examples of fragmented guidance for management of security risks in connected places include various reports such as: physical security measures for smart infrastructure (DSIT, 2022), the secure by design principles for IoT devices (UK Police Crime Prevention Initiatives, 2024), the security minded approach for smart cities (CPNI, 2017), the DSIT playbooks for secure connected places (DCMS, 2022b), the NCSC principles for cyber-security of connected places (NCSC, 2021b), existing regulations for connected places (National Protective Security Authority, 2023), the smart street manual (Transport Technology Forum, 2022), and existing guidance for managing the cybersecurity risks of CNI (NCSC, 2022b).
- iii. **Policy intervention:** There is a need for a clear policy intervention and a consistent framework for the security of connected places, one that is owned by a lead UK government department. This framework should also set the direction for the procurement and operation of smart services. The policy interventions need to align with the national cyber security strategy 2022-2030 which aims to develop capabilities for centralised governance to identify and oversee systemic cyber-security risks across sectors (NCSC, 2022c). A consistent methodology needs to be defined for identifying, assessing, monitoring, managing, and assuring systemic security risks (not just the IT risks) across multiple services owned and operated by different organizations within a connected place. The NCSC Capability Assessment Framework (CAF) could be enhanced and used for the assurance of cyber risks in connected places (DSIT, 2024b). Clear accountabilities, governance and assurance need to be defined and implemented to ensure that the cyber resilience specifications in contracts for smart services are adequate. DSIT’s governance in a box approach (DSIT, 2024b) provides generic process guidelines, but falls short of guidance for the governance of systemic security risks and events.
- iv. **Procurement of smart services:** UK Government’s reforms for the public procurement process could include the procurement of smart services within

connected places. For example, Innovation in procurement for London's authorities (LOTI, 2021), the Procurement guidance (Local Government Association, 2019) and Regulations 2024 (Legislation.gov.uk, 2024) could be joined up to help embed security-by-design in smart service procurement within UK's connected places.

- v. **Capability enhancements:** There could potentially be capability enhancements and structural changes to the LA's operating model for them to lead the way in the cyber risk assurance of smart infrastructure operations, rather than leaving private operators in a position of power. The NCSC connected place principles for cybersecurity, assurance framework for cyber resilience of connected places and DSIT guidance for secure connected places need to be enhanced. These enhancements should help define cyber resilience specifications and mitigations in smart service procurement frameworks and contracts. DSIT could include a gap analysis of connected place capabilities in their annual survey that assesses the national cybersecurity capabilities (DSIT, 2024a). Awareness sessions and training programmes need to be conducted to help the LAs define and meet capability roadmaps for assuring the security of connected urban places.

The UK Government's structure leads to responsibilities being spread across multiple departments and organizations, which can create challenges in determining which body or bodies should be responsible for implementing the recommendations outlined above. The researcher suggests that it would help if the UK Government could bring all organizations working on smart services (such as EV charging) under one umbrella, to bring some structure as well as visibility to the initiatives. As an example, Zenzic, a leading organization in the vehicle industry, has reached out to all relevant organizations within the UK to enable collaboration with each other and to understand the contribution of each organization to the UK Connected and Automated Mobility Roadmap to 2030 (Zenzic, 2022). The Government could possibly adopt a similar approach for equivalent technological advancements in other smart services, such as EV charging.

6.3 Limitations of this research

The study was limited by the small sample sizes and, inevitably, by a cut-off date for literature collection and interviews in a rapidly changing environment; and these factors should be considered when generalizing the findings. The comprehensiveness

of the results in the first stage of the research that studied the influence of urban elements on crime was limited by the number of studies that provided comparable effect sizes and the type of urban elements that were analysed in micro places. There were only eight urban elements that had sufficient data (with 1-8 effect sizes available) that could be combined for meta-analysis. It is important to note that the studies provided a correlation between urban elements and crime, this does not necessarily mean that one directly causes the other. Correlation only provides important aspects of relationships between two variables; it does not imply causation. Other factors, such as socio-demographic factors, and socioeconomic conditions could be contributing to the observed relationship. It is also worth noting that the review did not analyse the impact of security interventions introduced into urban environments, but rather focused solely on the effect of specific features or the presence of urban elements on crime. This distinction is important, as security measures and interventions could significantly influence crime rates and should be considered separately from the physical characteristics of urban spaces. Additionally, studies were not found that describe the influence of geo-tagged cyber activities of individuals, organizations, and government associated with digitally connected urban elements on physical crimes at micro places.

In the second stage of this study, where the cascading impacts of cyber-attacks on smart infrastructure were studied, the key limitation was that the academic literature on cascading impacts of cyber-attacks was small. This could be due to the delays associated with academic publishing, because of which the recent findings may not yet be in the public domain. As this research is a snapshot in time, it is possible that ongoing fast-paced innovations and emerging technologies could have changed or resolved the identified crime scenarios with cascading impacts, by the time these results are published. The cascading impacts of cyber-attacks could not be generalised (across use cases) as they were specific to the four infrastructure use cases that were selected.

Considering the third stage of the study, where the cyber-risks of connected places managed by the LAs in the procurement process of smart services was studied, only a sample of those involved were able to participate and it is possible that others might hold different views. Moreover, as the assessment was based on only one smart infrastructure use case (EV charging) implemented across seven city authorities within the UK, the findings are limited in these terms too and so should not be generalised to the whole of the UK or beyond. These are not unusual limitations, and they would

typically apply to any similar research, but they should be considered when interpreting the findings.

6.4 Recommended future research

This study has emphasised the need for more academic research into understanding the physical, cyber as well as cyber-physical criminogenic effects of urban elements on the continuously transforming crime and security landscape. The association between physical features of urban environments and the level of crime at places that are considered while re-designing-built environments aren't being studied continuously at the pace at which the urban infrastructure evolves. It has been highlighted that there is a need for more research to assess the association between physical features and the level of crime in micro places, as well as to explore how digital interactions and location-based online activities, associated with urban elements, might influence crime patterns in specific, localized urban areas. This research could provide deeper insights into the complex interplay between physical and digital factors in shaping crime dynamics in micro places. Understanding these dynamics could provide valuable insights into crime prevention strategies that consider both physical and digital environments. The impact of cyber enabled or cyber dependent activities/behaviours that influence urban crimes (such as online activities and the use of public WiFi) needs more attention, considering that the various digital products (such as drones and digital kiosks), infrastructure (such as smart roads), devices (such as smart phones, smart watches), and services (such as smart garbage collection) enabled by increasing internet connectivity are becoming more prevalent on streets. More research is also needed to assess the collective criminogenic influence of multiple types of urban elements in connected places and the impact of place managers.

There is also a lack of academic research on applying the principles of security and crime science in the same way as has been achieved through CPTED, to manage the security risks for overlapping physical and virtual elements of digitally connected built environments. Research needs to focus on comparable analysis of the quantitative effects of the evolving urban elements on crime at micro places. It is also important to study the crime concentration and variations in crime patterns in traditional physical micro places as well as digitally connected environments to assess the influence of existing and emerging urban elements on crime. The principles of

environment criminology could be applied to analyse the inherent criminogenic properties of the smart features of digital urban elements (e.g., inappropriate use of smart surveillance, potential misuse of drones for spying on people, misuse of location-based systems to track people) and their impacts on the routine activities of people (such as changing the journey routes to avoid areas where there are surveillance cameras). The analysis could focus on strategies for predicting how these transformations might impact security risks and how to address the identified issues. The five principles of Situational Crime Prevention (increasing effort, reducing rewards environments and, removing excuses, and reducing provocations) need to be re-interpreted in terms of reducing crime opportunities in virtual and smart environments, and helping to enhance the security interventions built within the urban ecosystem. More research is required on crime and place for cybercrimes, smart initiatives and connected places. The role of controllers and super controllers is spread across multiple entities in traditional physical, cyber and cyber-physical (i.e. connected) places. These roles need to be redefined and expanded to create synergies across physical, cyber, and hybrid environments, ensuring they can adapt to the evolving complexity of secure connected environments. The goal is to enable integrated governance that ensures security, efficiency, and resilience in managing both physical infrastructure and digital systems within connected places.

Further research could build upon the findings and recommendations of this study to assess the risks and mitigations of potential systemic events and cascading impacts in the street environment to protect the CNI. The implementation of 'security and resilience by design' within the procurement of smart infrastructure services from private operators needs to be researched further. This research could be extended by expanding the scope to include more elements of connected places and a broader range of stakeholders. Academic research is also needed to map the principles of resilience by design to the systemic risks that can feed into cyber insurance policies - which is also an under researched area. Additionally, there is a need for more continuous research to critically examine the potential misuse of connected street infrastructure that can target the CNI.

6.5 Impact of this doctoral research

The aim of this study was achieved by exploring key challenges related to the impact of urban changes on crime and security in three distinct stages: 1) analysis of physical

crime patterns linked to traditional urban elements, 2) assessment of digital infrastructure integration with traditional urban elements and its criminogenic impacts on CNI in connected street environments, and 3) evaluation of effectiveness of LAs (place managers) and Government (super controllers) in securing connected places right from the procurement stage of smart infrastructure. The thesis offers vital insights for integrating security and resilience into urban planning, ensuring cities are prepared for the challenges of a digital, interconnected world. It also contributes to crime and place literature and informs policy development to address evolving security risks in connected spaces.

This study identified gaps in the application of environment criminology theories to the overlapping physical and digital environments – environments in which crimes are evolving at a fast pace. The research and recommendations of this thesis have been published in an academic journal, a deliverable for European Union Horizon 2020 project and a policy paper; the research was also presented in multiple conferences (see Chapter 1, Section 1.4).

This study provided insights into a) the scale of the overall issues observed in the implementation of NCSC guidelines, and the resulting risk exposures in connected places, b) an understanding of how to address the challenges faced and c) whether the NCSC connected places guidelines for cybersecurity are fit for purpose. The participants for this study in the UK included organizations from public sector (6 Local Authorities - LAs, Transport for London(tfL)), Government of the UK (DfT, DSIT, NCSC) and private sector operators. The early findings from this study, including identified gaps in governance guidelines for the cybersecurity of connected places, were used to shape the scope of a government-funded Alpha Testing project, where Local Authorities (LAs) were invited to test the guidance on cybersecurity for Connected Places. This project was established by DSIT to understand how LAs can be supported to implement the NCSC cybersecurity principles for connected places. Additionally, the Department of Transport and the Connected Places Catapult took on board the finding that there was a lack of cyber resilience risk management within the new smart streets manual. They included common cybersecurity guidance for use-cases within the smart street manual. The study also had an impact on LAs. For example, after discussing the interview questionnaire with the researcher, one of the LAs involved in the interviews included a requirement for business continuity dry runs in the procurement contract specifications that they employ.

The study emphasised the need for establishing ‘security and resilience by design’ to protect the CNI in the continuously developing connected places by countering the cascading impacts of smart infrastructure. It then provided inputs to the UK Government for the formulation of national policy applicable to the security of connected places in a way that it is implementable at the local level. Its findings can inform city authorities, governments, and urban planners about the key issues involved in implementing, governing, and assuring the security interventions needed to counter the evolving crimes risks on smart urban infrastructure and its cascading impacts in the street environment. The findings can also help to provide practical guidance in anticipating criminogenic properties as further innovations (such as the anticipated connected automated vehicles) are rolled out in connected places. Recommendations were provided for enhancing Government guidelines to manage new systemic risks within the connected street environment, which would also help to address systemic vulnerabilities as prioritised in the NCSC cybersecurity strategy 2022-2030.

The published academic article and policy paper produced from this thesis were sent to all the stakeholders involved in the research and were received positively. DSIT and NCSC were also engaged to brainstorm what actions need to be taken to address the findings and implement the recommendations specific to improvements in policy and guidelines. The UK Government’s Connected places policy teams engaged with the researcher and have taken on board some of the recommendations. For example, the fragmented DSIT and NCSC guidance for secure connected places has been consolidated and published on a common website (DCMS, 2021). DSIT commissioned a review of global approaches and policies for cybersecurity of connected places (Plexal on behalf of DSIT, 2023). The research also has the potential to have further impact, as it is aligned with UK Government’s cyber security objectives.

References

- Abbu, H. R., Fleischmann, D., & Gopalakrishna, P. (2021). The Digital Transformation of the Grocery Business - Driven by Consumers, Powered by Technology, and Accelerated by the COVID-19 Pandemic. *Advances in Intelligent Systems and Computing*, 1367 AISC, 329–339. https://doi.org/10.1007/978-3-030-72660-7_32/COVER
- Abrams, D. S. (2021). COVID and crime: An early empirical look. *Journal of Public Economics*, 194, 104344. <https://doi.org/10.1016/j.jpubeco.2020.104344>
- Acharya, Dvorkin, Y., & Karri, R. (2020). Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable? *IEEE Transactions on Smart Grid*, 11(6), 5099–5113. <https://doi.org/10.1109/TSG.2020.2994177>
- Acharya, S., Dvorkin, Y., Pandzic, H., & Karri, R. (2020). Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective. *IEEE Access*, 8, 214434–214453. <https://doi.org/10.1109/ACCESS.2020.3041074>
- ACN Newswire. (2015). *National Security Strategy and Strategic Defence and Security Review*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478936/52309_Cm_9161_NSS_SD_Review_PRINT_only.pdf
- Adams, G. T. (2016). *EMPOWERING CONSUMERS AS CAPABLE GUARDIANS TO PREVENT ONLINE PRODUCT COUNTERFEITING VICTIMIZATION IN THE ATHLETIC FOOTWEAR INDUSTRY: A ROUTINE ACTIVITY PERSEPCTIVE*. Michigan State University.
- Adel, H., Salheen, M., & Mahmoud, R. A. (2016). Crime in relation to urban design. Case study: The Greater Cairo Region. *Ain Shams Engineering Journal*, 7(3), 925–938. <https://doi.org/10.1016/J.ASEJ.2015.08.009>
- Ahmed, M. A., & Kim, Y. C. (2017). Performance analysis of communication networks for EV charging stations in residential grid. *DIVANet 2017 - Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications, Co-Located with MSWiM 2017*, 63–70. <https://doi.org/10.1145/3132340.3132352>
- Ahmed, S. H., & Rani, S. (2018). A hybrid approach, Smart Street use case and future aspects for Internet of Things in smart cities. *Future Generation Computer Systems*, 79, 941–951. <https://doi.org/10.1016/j.future.2017.08.054>
- Alba, A. R., & Linsangan, N. B. (2022). Application Specific Computer for Intelligent Monitoring of Cabled Streetlights with Theft Detection Features. *2022 IEEE 14th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)*, 1–6.
- Alcaraz, C., Cumplido, J., & Triviño, A. (2023). OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0. *International Journal of Information Security*, 22(5), 1395–1421. <https://doi.org/10.1007/s10207-023-00698-8>

- Almeida, V. A. F., Doneda, D., & Moreira da Costa, E. (2018). Humane Smart Cities: The Need for Governance [Article]. *IEEE Internet Computing*, 22(2), 91–95. <https://doi.org/10.1109/MIC.2018.022021671>
- Alvarez, R., Duarte, F., Frenchman, D., & Ratti, C. (2022). Sensing Lights: The Challenges of Transforming Street Lights into an Urban Intelligence Platform. *Journal of Urban Technology*, 29(4), 25–40. <https://doi.org/10.1080/10630732.2022.2082825>
- Alves, D., Martinez, L. M., & Viegas, J. M. (2012). Retrieving real-time information to users in public transport networks: an application to the Lisbon bus system. *Procedia-Social and Behavioral Sciences*, 54, 470–482.
- Ambrosino, G., Nelson, J. D., Boero, M., & Pettinelli A A Memex, I. (2016). *Enabling intermodal urban transport through complementary services: From Flexible Mobility Services to the Shared Use Mobility Agency Workshop 4. Developing inter-modal transport systems*. <https://doi.org/10.1016/j.retrec.2016.07.015>
- Amram, S., Weisburd, D., & Shay, M. (2024). Examining Crime-Specific and Crime-General Theories of Crime Causation at Place: The Case of Property and Violent Crime on Street Segments in Tel Aviv-Yafo. *International Annals of Criminology*, 62(1), 8–29. <https://doi.org/10.1017/cri.2024.1>
- Anderson, R. (2008). Network Attack and Defense. *Security Engineering*, 633–678.
- Andrade, R. O., Yoo, S. G., Tello-Oquendo, L., & Ortiz-Garcés, I. (2021). Cybersecurity, sustainability, and resilience capabilities of a smart city [Bookitem]. In *Smart Cities and the UN SDGs* (pp. 181–193). <https://doi.org/10.1016/B978-0-323-85151-0.00012-9>
- Andrysiak, T., Saganowski, Ł., & Kiedrowski, P. (2017). Predictive Abuse Detection for a PLC Smart Lighting Network Based on Automatically Created Models of Exponential Smoothing [Article]. *Security and Communication Networks*, 2017, 1–13; 13. <https://doi.org/10.1155/2017/7892182>
- Antoun, J., Kabir, M. E., Moussa, B., Atallah, R., & Assi, C. (2020). A Detailed Security Assessment of the EV Charging Ecosystem. *IEEE Network*, 34(3), 200–207. <https://doi.org/10.1109/MNET.001.1900348>
- Armitage, R. (2011). *The Impact of Connectivity and Through-Movement within Residential Developments on Levels of Crime and Anti-Social Behaviour Original Citation*. <http://eprints.hud.ac.uk/id/eprint/13592/>
- Armitage, R. (2013). Exploring the Theoretical Links between Design and Crime. In *Crime Prevention through Housing Design* (pp. 9–26). Palgrave Macmillan UK. https://doi.org/10.1057/9781137316059_2
- Armitage, R. (2018). Burglars' take on crime prevention through environmental design (CPTED): Reconsidering the relevance from an offender perspective. *Security Journal*, 31(1), 285–304. <https://doi.org/10.1057/s41284-017-0101-6>
- Armitage, R., & Monchuk, L. (2019a). What Is CPTED? Reconnecting Theory with Application in the Words of Users and Abusers. *Policing: A Journal of Policy and Practice*, 13(3), 312–330. <https://doi.org/10.1093/police/pax004>
- Armitage, R., & Monchuk, L. (2019b). What Is CPTED? Reconnecting Theory with

- Application in the Words of Users and Abusers. *Policing: A Journal of Policy and Practice*, 13(3), 312–330. <https://doi.org/10.1093/police/pax004>
- Armitage, R., & Pease, K. (2008). Predicting and Preventing the Theft of Electronic Products. *European Journal on Criminal Policy and Research*, 14(1), 11–37. <https://doi.org/10.1007/s10610-007-9039-2>
- Arshad, M. H., Bilal, M., & Gani, A. (2022). Human Activity Recognition: Review, Taxonomy and Open Challenges. *Sensors*, 22(17), 6463. <https://doi.org/https://doi.org/10.3390/s22176463>
- Ashby, M. (2019). *Studying Crime and Place with the Crime Open Database* [Article].
- Ashour, R., Taha, T., Mohamed, F., Hableel, E., Kheil, Y. A., Elsalamouny, M., Kadadha, M., Rangan, K., Dias, J., Seneviratne, L., & Cai, G. (2016). Site inspection drone: A solution for inspecting and regulating construction sites. *Midwest Symposium on Circuits and Systems*, 0. <https://doi.org/10.1109/MWSCAS.2016.7870116>
- Atkins, S., Husain, S., & Storey, A. (1991). *THE INFLUENCE OF STREET LIGHTING ON CRIME AND FEAR OF CRIME*. <http://www.celfosc.org/biblio/seguridad/atkins.pdf>
- Atlas, R. I. (2008). *21st century security and CPTED: designing for critical infrastructure protection and crime prevention*. CRC Press. <https://search-proquest-com.libproxy.ucl.ac.uk/docview/199685445?accountid=14511%0A>
- Australian Bureau of Statistics. (2016). *2901.0 - Census of Population and Housing: Census Dictionary, 2016*. <https://www.abs.gov.au/ausstats/abs@.nsf/Lookup/2901.0Chapter23002016>
- Avery, D. (2023). *Cyber Attackers are Coming for Transit Agencies, Here's How to Strengthen Your Security Posture*. Mass Transit. <https://www.masstransitmag.com/safety-security/article/53068710/cyber-attackers-are-coming-for-transit-agencies-heres-how-to-strengthen-your-security-posture>
- Ayres, L. (2007). Qualitative research proposals-Part I: Posing the problem. *Journal of Wound, Ostomy and Continence Nursing*, 34(1), 30–32. <https://doi.org/10.1097/00152192-200701000-00004>
- Baba, M., Gui, V., Cernazanu, C., & Pescaru, D. (2019). A Sensor Network Approach for Violence Detection in Smart Cities Using Deep Learning. *Sensors 2019, Vol. 19, Page 1676*, 19(7), 1676. <https://doi.org/10.3390/S19071676>
- Back, S., & Guerette, R. T. (2021). Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks. *Journal of Contemporary Criminal Justice*, 37(3), 427–451. <https://doi.org/10.1177/10439862211001628>
- Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., Sansurooah, K., Syed, N., & Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, 22, 3–13. <https://doi.org/10.1016/J.DIIN.2017.06.015>
- Baker, J. D. (2016). The purpose, process, and methods of writing a literature review.

AORN Journal, 103(3), 265–269.

- Barau. (2016). Cyber insecurity as a manifestation of new form of global urban vulnerability. *Imam Journal of Applied Sciences*, 1(1), 27. <http://www.e-ijas.org/article.asp?issn=WKMP-0143;year=2016;volume=1;issue=1;spage=27;epage=32;aulast=Barau>
- Barnfield, P. (2020, June 1). *High Streets beware the digital gap (Part 2)*. LinkedIn. <https://www.linkedin.com/pulse/high-streets-beware-digital-gap-part-2-polly-barnfield-obe/>
- Barns, S., Cosgrave, E., Acuto, M., & McNeill, D. (2016). *Digital Infrastructures and Urban Governance* [Article].
- Barr, R., & Pease, K. (1990). Crime Placement, Displacement, and Deflection. *Crime and Justice*, 12, 277–318. <https://doi.org/10.1086/449167>
- Barr, S., Lampkin, S., Dawkins, L., & Williamson, D. (2021). Smart cities and behavioural change:(Un) sustainable mobilities in the neo-liberal city. *Geoforum*, 125, 140–149.
- Barthélemy, J., Verstaeevel, N., Forehead, H., & Perez, P. (2019). Edge-Computing Video Analytics for Real-Time Traffic Monitoring in a Smart City [Article]. *Sensors (Basel, Switzerland)*, 19(9), 2048. <https://doi.org/10.3390/s19092048>
- Basnet, M., & Ali, M. H. (2021). Exploring cybersecurity issues in 5G enabled electric vehicle charging station with deep learning. *IET Generation, Transmission & Distribution*, 15(24), 3435–3449.
- Bauer, Sanchez, L., & Song, J. (2021). IoT-Enabled Smart Cities: Evolution and Outlook. In *Sensors* (Vol. 21, Issue 13). <https://doi.org/10.3390/s21134511>
- Beavon, D. J. K., Brantingham, P. L., & Brantingham, P. J. (1994). *THE INFLUENCE OF STREET NETWORKS ON THE PATTERNING OF PROPERTY OFFENSES*. http://www.popcenter.org/library/crimeprevention/volume_02/06beavon.pdf
- Beccali, M., Bonomolo, M., Galatioto, A., & Pulvirenti, E. (2017). Smart lighting in a historic context: A case study. *Management of Environmental Quality*, 28(2), 282–298. <https://doi.org/10.1108/meq-06-2015-0109>
- Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023). A Review of Colonial Pipeline Ransomware Attack. *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 8–15. <https://doi.org/10.1109/CCGridW59191.2023.00017>
- Bendler, J., Ratku, A., & Neumann, D. (2014). Crime mapping through geo-spatial social media activity. *35th International Conference on Information Systems "Building a Better World Through Information Systems", ICIS 2014*.
- Benedict, T. . (2022). The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest [Article]. *Washington and Lee Law Review*, 79(2), 849–898.
- Bernasco, W, Ruiter, S., & Johnson, S. (2015). Learning where to offend: Effects of past on future burglary locations [Article]. *Applied Geography* , 60 120 - 129. (2015).

- Bernasco, Wim. (2010). A SENTIMENTAL JOURNEY TO CRIME: EFFECTS OF RESIDENTIAL HISTORY ON CRIME LOCATION CHOICE [Article]. *Criminology (Beverly Hills)*, 48(2), 389–416. <https://doi.org/10.1111/j.1745-9125.2010.00190.x>
- Bernasco, Wim, & Block, R. (2011). Robberies in Chicago: A Block-Level Analysis of the Influence of Crime Generators, Crime Attractors, and Offender Anchor Points. *Journal of Research in Crime and Delinquency*, 48(1), 33–57. <https://doi.org/10.1177/0022427810384135>
- Bharatiraja, C., Padmanaban, S., Siano, P., Krishnamoorthy, R., & Selvaraj, R. (2017). Real-time forecasting of EV charging station scheduling for smart energy systems. *Energies*, 10(3). <https://doi.org/10.3390/EN10030377>
- Biswal, A. K., Singh, D., & Pattanayak, B. K. (2021). *IoT-Based Voice-Controlled Energy-Efficient Intelligent Traffic and Street Light Monitoring System BT - Green Technology for Smart City and Society* (Renu Sharma, M. Mishra, J. Nayak, B. Naik, & D. Pelusi (Eds.); pp. 43–54). Springer Singapore.
- Bitnik, M. (2014). Surveillance Chess. *Surveillance & Society*, 12(3), 459–465.
- Blackman, J. (2020). *Smart Lighting as a platform*. RCR Wireless News. <https://www.rcrwireless.com/20200320/internet-of-things/smart-lighting-as-a-platform-to-attack-inefficiency>
- Blackwell, T. (2022, March 24). *London's future as a smart city*. Centre For London. <https://www.centreforlondon.org/blog/londons-future-as-a-smart-city/>
- Blancaflor, E., Ong, A. P., Navarro, A. L. E., Sudo, K. F., & Villasor, D. A. (2023). Exploring the Attacks, Impacts, and Mitigations in a Real-Time Streaming Protocol Service of IP Cameras. *Proceedings of the 2023 9th International Conference on Computer Technology Applications*, 201–205.
- Block, R. L., & Block, C. B. (2000). *The Bronx and Chicago: street robbery in the environs of rapid transit stations BT - Analyzing crime patterns: frontiers of practice* (V. Goldsmith, P. McGuire, J. Mellkopf, & T. Ross (Eds.)). Sage Publications Inc.
- Blythe, J. M., & Johnson, S. D. (2021). A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal*, 34(1), 97–125. <https://doi.org/10.1057/S41284-019-00211-8/TABLES/4>
- Blythe, J. M., Johnson, S. D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Science*, 9(1), 1–9. <https://doi.org/10.1186/s40163-019-0110-3>
- Boessen, A., Hipp, J. R., & Boessen, A. (2018). Parks as crime inhibitors or generators: Examining parks and the role of their nearby context. *Social Science Research*, 76, 186–201. <https://doi.org/10.1016/j.ssresearch.2018.08.008>
- Borbely, D., Gehrsitz, M., McIntyre, S., & Rossi, G. (2023). *Permanent school closures and crime: evidence from Scotland*. Department of Economics, University of Sheffield.
- Borenstein, M., Hedges, L. V., Higgins, J. P. T., & Rothstein, H. R. (2010). A basic introduction to fixed-effect and random-effects models for meta-analysis.

Research Synthesis Methods, 1(2), 97–111. <https://doi.org/10.1002/jrsm.12>

- Bowers, K. (2014). Risky Facilities: Crime Radiators or Crime Absorbers? A Comparison of Internal and External Levels of Theft. In *Source: Journal of Quantitative Criminology* (Vol. 30, Issue 3).
- Bowers, K. J., Johnson, S. D., Guerette, R. T., Summers, L., & Poynton, S. (2011). Spatial displacement and diffusion of benefits among geographically focused policing initiatives: A meta-analytical review. *Journal of Experimental Criminology*, 7(4), 347–374. <https://doi.org/10.1007/S11292-011-9134-8>
- Bowers, K. J., Johnson, S. D., & Pease, K. (2004). PROSPECTIVE HOT-SPOTTING: The Future of Crime Mapping? *Source: The British Journal of Criminology*, 44(5), 641–658. <https://doi.org/10.1093/bjc/azh036>
- Bowers, K., Johnson, S., Guerette, R. T., Summers, L., & Poynton, S. (2011). SPATIAL DISPLACEMENT AND DIFFUSION OF BENEFITS AMONG GEOGRAPHICALLY FOCUSED POLICING INITIATIVES. *Campbell Systematic Reviews*, 7(1), 1–144. <https://doi.org/10.4073/csr.2011.3>
- Braga, A. A., Papachristos, A. V., & Hureau, D. M. (2014). The Effects of Hot Spots Policing on Crime: An Updated Systematic Review and Meta-Analysis. *Justice Quarterly*, 31(4), 633–663. <https://doi.org/10.1080/07418825.2012.673632>
- Brantingham, P., & Brantingham, P. (2013). Crime pattern theory. In *Environmental Criminology and Crime Analysis* (pp. 78–94). https://ucl-new-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=TN_scopus2-s2.0-84906163648&context=PC&vid=UCL_VU2&lang=en_US&search_scope=CSCO_P_UCL&adaptor=primo_central_multiple_fe&tab=local&query=any,contains,Brantham 1993 crime patte
- Brantingham, Patricia, & Brantingham, P. (1995). Criminality of place Crime generators and crime attractors. *European Journal on Criminal Policy and Research*, 3(3), pages5–26.
- Brighente, A., Conti, M., Donadel, D., Poovendran, R., Turrin, F., & Zhou, J. (2023). Electric Vehicles Security and Privacy: Challenges, Solutions, and Future Needs. *ArXiv Preprint ArXiv:2301.04587*.
- Bruinsma, G. J. N., Johnson, S. D., Llinares, F. M., & Johnson, S. D. (2018). *Cybercrime and PlaceApplying Environmental Criminology to Crimes in Cyberspace*. Oxford University Press.
- BSI Standards Publication PAS 181:2014. (2014). <https://shop.bsigroup.com/upload/283889/PAS-181.pdf>
- Buil-Gil, D., & Saldaña-Taboada, P. (2022). Offending Concentration on the Internet: An Exploratory Analysis of Bitcoin-related Cybercrime. *Deviant Behavior*, 43(12), 1453–1470. <https://doi.org/10.1080/01639625.2021.1988760>
- Burke, W., Stranieri, A., Oseni, T., & Gondal, I. (2024). The need for cybersecurity self-evaluation in healthcare. *BMC Medical Informatics and Decision Making*, 24(1), 133. <https://doi.org/10.1186/s12911-024-02551-x>
- Bushman, Brad J, & Wang, M. C. (2009). Vote-counting procedures in meta-analysis.

- In *The Hand. of Res. Synthesis and Meta-Analysis, 2nd Ed* (pp. *The Hand. of Res. Synthesis and Meta-Analysis, 2nd Ed*, 2009). https://www.researchgate.net/publication/285464887_Vote-counting_procedures_in_meta-analysis
- Butkovic, A., Mrdovic, S., Uludag, S., & Tanovic, A. (2019). Geographic profiling for serial cybercrime investigation. *Digital Investigation*, 28, 176–182. <https://doi.org/10.1016/j.diin.2018.12.001>
- Butler, C. (2013). What constitutes success? A critical review of the practice and implementation of Crime Prevention through Environmental Design in New Zealand. *Safer Communities*, 12. <https://doi.org/10.1108/SC-06-2013-0007>
- Campbell Collaboration. (2020). *Campbell Collaboration*. <https://www.campbellcollaboration.org/about/>
- Cancelado, C. M. (n.d.). *Coordinated Street Furniture Franchise (CSFF) New York City*.
- Candelieri, A., Galuzzi, B. G., Giordani, I., & Archetti, F. (2019). Vulnerability of public transportation networks against directed attacks and cascading failures. *Public Transport*, 11(1), 27–49. <https://doi.org/10.1007/S12469-018-00193-7/FIGURES/12>
- Card, A. J. (2017). The problem with ‘5 whys.’ *BMJ Quality & Safety*, 26(8), 671–677. <https://doi.org/10.1136/BMJQS-2016-005849>
- Carey, C. (2022). *EV charging points hacked to show explicit material*. CitiesToday. <https://cities-today.com/ev-charging-points-hacked-to-show-explicit-material/>
- Careya, C. (2022). *Major UK bus operator hit by cyber attack*. Cities Today. <https://cities-today.com/major-uk-bus-operator-hit-by-cyber-attack/>
- Carroll, T. E., Dindlebeck, G. B., Pratt, R. M., & O’Neil, L. R. (2022). *A Threat Model of High-Power Electric Vehicle Charging Infrastructure*.
- CBS News. (2016, January). *New York City phone booths transformed into Wi-Fi hotspots*. . . <https://www.cbsnews.com/news/phone-booths-transformed-into-wi-fi-hotspots/>
- Ceccato, V. (2012). The Urban Fabric of Crime and Fear. In V. Ceccato (Ed.), *The Urban Fabric of Crime and Fear* (pp. 1–33). Springer Netherlands. https://doi.org/10.1007/978-94-007-4210-9_1
- Census Information. (2010). *Understanding Census Geography - United States*. University of Pittsburgh. <https://pitt.libguides.com/uscensus/understandinggeography>
- Cerrudo, C. (2015). An emerging US (and world) threat: Cities wide open to cyber attacks. *Securing Smart Cities*, 17(2015), 137–151.
- Chainey, S., & Ratcliffe, J. (2005). *GIS and crime mapping*. Wiley.
- Chainey, S., Tompson, L., & Uhlig, S. (2008). The Utility of Hotspot Mapping for Predicting Spatial Patterns of Crime. *Security Journal*, 21(1–2), 4–28. <https://doi.org/10.1057/palgrave.sj.8350066>

- Chan, C. (2023). *The Rise of CCTV Hacks in an Evolving Cyber-Threat Landscape*. Infosecurity Magazine. <https://www.infosecurity-magazine.com/opinions/rise-cctv-hacks-cyber-threat/>
- Chaudhuri, A., & Bozkus Kahyaoglu, S. (2023). CYBERSECURITY ASSURANCE IN SMART CITIES: A RISK MANAGEMENT PERSPECTIVE. *EDPACS*, 1–22. https://doi.org/10.1080/07366981.2023.2165293/SUPPL_FILE/UEDP_A_2165293_SM2253.PDF
- Chen, T., Zhang, X.-P., Wang, J., Li, J., Wu, C., Hu, M., & Bian, H. (2020). A review on electric vehicle charging infrastructure development in the UK. *Journal of Modern Power Systems and Clean Energy*, 8(2), 193–205.
- Cheng, F. (2011). Security Attack Safe Mobile and Cloud-based One-time Password Tokens Using Rubbing Encryption Algorithm. *Mobile Networks and Applications; New York*, 16(3), 304–336. <https://doi.org/10.1007/s11036-011-0303-9>
- Chiara, P. G. (2022). The IoT and the new EU cybersecurity regulatory landscape [Article]. *International Review of Law, Computers & Technology*, 36(2), 118–137. <https://doi.org/10.1080/13600869.2022.2060468>
- Chief Digital Officer for London. (2018). *How the ‘humble lamppost’ means smarter streets — through London’s big collaboration with fellow European cities*. Medium. <https://chiefdigitalofficer4london.medium.com/the-humble-lamppost-means-smarter-streets-through-london-s-big-collaboration-with-fellow-european-f3f25975c93e>
- Cho, Y., Jeong, H., Choi, A., & Sung, M. (2019). Design of a Connected Security Lighting System for Pedestrian Safety in Smart Cities. In *Sustainability* (Vol. 11, Issue 5). <https://doi.org/10.3390/su11051308>
- Chockalingam, S., & Maathuis, C. (2022). *Assessing Cascading Effects of Cyber-Attacks in Interconnected Critical Infrastructures*.
- Chris Lewis Group. (2021). *Cybersecurity and CCTV*. <https://www.chrislewis.co.uk/blog/cyber-security-and-cctv>
- Chynoweth, J., Chung, C.-Y., Qiu, C., Chu, P., & Gadh, R. (2014). Smart electric vehicle charging infrastructure overview. *ISGT 2014*, 1–5.
- CISA. (2021). *Systemic Cyber Risk Reduction*. CISA.Gov, An Official Website of the U.S. Department of Homeland Security. <https://www.cisa.gov/resources-tools/programs/systemic-cyber-risk-reduction>
- Clancey, G., Fisher, D., & Rutherford, A. (2014). An exploratory study of crime risks and the planning process [Article]. *Crime Prevention and Community Safety*, 16(1), 1–19. <https://doi.org/10.1057/cpcs.2013.13>
- Clancey, G., Lee, M., & Fisher, D. (2012). Crime prevention through environmental design (CPTED) and the New South Wales crime risk assessment guidelines: A critical review. In *Crime Prevention and Community Safety* (Vol. 14, Issue 1, pp. 1–15). <https://doi.org/10.1057/cpcs.2011.10>
- Clancey, G., Monchuk, · Leanne, Anderson, J., & Ellis, J. (2018). Lost in implementation: NSW police force crime prevention officer perspectives on crime prevention through environmental design. *Crime Prev Community Saf*, 20, 139–

153. <https://doi.org/10.1057/s41300-018-0043-x>

- Clarion Security Systems. (2022). *How many CCTV cameras are in London?* <https://clarionuk.com/resources/how-many-cctv-cameras-are-in-london/#:~:text=in the UK%3F-,Research by Clarion Security Systems estimates that there are over,cameras in the UK varies.>
- Clark James, & Cook David. (2022, December 5). *UK NIS – Get ready for expansion of the UK's critical national infrastructure cyber security laws – Privacy Matters*. DLA Piper. <https://blogs.dlapiper.com/privacymatters/uk-nis-get-ready-for-expansion-of-the-uks-critical-national-infrastructure-cyber-security-laws/>
- Clarke, R., and J. E. (2005). *Crime Analysis for Problem Solvers—In 60 Small Steps*. Office of Community Oriented Policing Services (COPS) Washington, DC 20530. <https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=232576>
- Clarke, R. V., & Cornish, D. (1985). Modeling offenders' decisions: A framework for research and policy. *Chicago Journals*, 6, 147–185.
- Clarke, R. V. G., & Felson, M. (1993). *Routine Activity and Rational Choice*.
- Clarke, R. V. G., & Mayhew, P. (1980). *Designing out crime / edited by R.V.G. Clarke and P. Mayhew, Home Office Research Unit*. London : H.M.S.O.
- Clarke, R. V. (1983). Situational Crime Prevention: Its Theoretical Basis and Practical Scope. In *Crime and Justice* (Vol. 4, pp. 225–256). The University of Chicago Press. <https://doi.org/10.2307/1147510>
- Clarke, R. V. (1997). *Situational Crime Prevention Successful Case Studies Second Edition*.
- Clarke, R. V., & Weisburd, D. (1994). *DIFFUSION OF CRIME CONTROL BENEFITS: OBSERVATIONS ON THE REVERSE OF DISPLACEMENT*.
- Clim, A., Toma, A., Zota, R. D., & Constantinescu, R. (2023). The Need for Cybersecurity in Industrial Revolution and Smart Cities. In *Sensors* (Vol. 23, Issue 1). <https://doi.org/10.3390/s23010120>
- Clough, J. (2015). Principles of cybercrime, second edition. In *Principles of Cybercrime, Second Edition*. Cambridge University Press. <https://doi.org/10.1017/CBO9781139540803>
- Clutter, J. E., Henderson, S., & Haberman, C. P. (2019). The Impact of Business Improvement District Proximity on Street Block Robbery Counts. *Crime & Delinquency*, 65(8), 1050–1075. <https://doi.org/10.1177/0011128719834559>
- Cohen, L. E., & Felson, M. (1979a). Social Change and Crime Rate Trends: A Routine Activity Approach. In *Source: American Sociological Review* (Vol. 44, Issue 4).
- Cohen, L. E., & Felson, M. (1979b). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), 588. <https://doi.org/10.2307/2094589>
- Cohn, L. D., & Decker, B. J. (2003). How Meta-Analysis Increases Statistical Power. In *Psychological Methods* (Vol. 8, Issue 3, pp. 243–253). <https://doi.org/10.1037/1082-989X.8.3.243>

- Colenbrander, S., & Barau, A. (2019). Planning and financing urban development in the context of the climate crisis. In *International Journal of Urban Sustainable Development* (Vol. 11, Issue 3, pp. 237–244). Taylor and Francis Inc. <https://doi.org/10.1080/19463138.2019.1673529>
- Coletta, C., Heaphy, L., & Kitchin, R. (2019). From the accidental to articulated smart city: The creation and work of 'Smart Dublin' [Article]. *European Urban and Regional Studies*, 26(4), 349–364. <https://doi.org/10.1177/0969776418785214>
- Connected Places Catapult. (2021). *NEUROSCIENCE: A Playbook for Placemakers*.
- Conti, M., Donadel, D., Poovendran, R., & Turrin, F. (2022). Evexchange: A relay attack on electric vehicle charging system. *European Symposium on Research in Computer Security*, 488–508. https://link.springer.com/chapter/10.1007/978-3-031-17140-6_24
- Coolfire. (2018). *THE STREET LIGHT OF THE FUTURE WILL BE CONNECTED*. Coolfire Blog. <https://www.coolfiresolutions.com/blog/smart-street-lights/>
- COORAY, M., DUUS, R., & BUNDGAARD, L. (2016). *Connected Cities: Driving Digital Transformation in Complex Ecosystems*. Future of Cities, UCL. https://www.mgmt.ucl.ac.uk/sites/default/files/upload/TEBR_NovDec_Connected_Cities-Driving_Digital_Transformation_in_Complex_Ecosystems.pdf
- Cornish, D. B., & Clarke, R. V. (1987). UNDERSTANDING CRIME DISPLACEMENT: AN APPLICATION OF RATIONAL CHOICE THEORY. *Criminology*, 25(4), 933–948. <https://doi.org/10.1111/j.1745-9125.1987.tb00826.x>
- Corso, A. J., & Monday, M. B. A. (2015). *A Three-Part Exploration Linking Social Media, Big Data, and GIS: A Case of Predictive Crime Analysis*. The Claremont Graduate University.
- Costelloe, K. (2019). Amazon Selects Irvine For Scout Robot Delivery. *Orange County Business Journal*, 42(33), 4.
- Costin, A. (2016). Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations. *Proceedings of the 6th International Workshop on Trustworthy Embedded Devices*, 45–54. <https://doi.org/10.1145/2995289.2995290>
- Covington, M. J., & Carskadden, R. (2013). *Threat Implications of the Internet of Things*.
- Cozens, P., & Love, T. (2015). A Review and Current Status of Crime Prevention through Environmental Design (CPTED). *Journal of Planning Literature*, 30(4), 150–412. <https://doi.org/10.1177/0885412215595440>
- Cozens, P., Love, T., & Davern, B. (2019). Geographical juxtaposition: A new direction in CPTED. *Social Sciences*, 8(9). <https://doi.org/10.3390/socsci8090252>
- Cozens, P M. (2002). Sustainable Urban Development and Crime Prevention Through Environmental Design for the British City. Towards an Effective Urban Environmentalism for the 21st Century. In *Cities* (Vol. 19, Issue 2). www.elsevier.com/locate/cities
- Cozens, Paul Michael, Saville, G., & Hillier, D. (2005). Crime prevention through

- environmental design (CPTED): a review and modern bibliography. *Property Management*, 23(5), 328–356. <https://doi.org/10.1108/02637470510631483>
- CPNI. (2022, February). *Security-Minded approach to developing Smart Cities* | CPNI. <https://www.cpni.gov.uk/security-minded-approach-developing-smart-cities>
- CPNI, B. (2017). *PAS 185:2017 Smart Cities - Specification for establishing and implementing a security-minded approach*. https://www.cpni.gov.uk/system/files/documents/4e/b0/PAS_185_2017_Introduction_Smart_Cities.pdf
- Crowe, T. D. (2000). *Crime Prevention Through Environmental Design - Timothy Crowe, NCPI - Google Books*. https://books.google.co.uk/books?hl=en&lr=&id=prgIS7CH9F8C&oi=fnd&pg=PR11&ots=54mJmIAZyc&sig=xKMgE40JoSmfpiVMOOrqKZCrmAc&redir_esc=y#v=onepage&q&f=false
- Cunningham, C., Hannon, C., Malik, M., Paik, R., Paramesh, R., Samford, H., Sangcharoenvanakul, K., Sanguinet, S., Wattles, A., Wirth, A., Anderson, A., & Beyer, J. (2018). *ADDRESSING SYSTEMIC CYBERSECURITY RISK APPLIED RESEARCH PROGRAM*. <http://jsis.uw.edu/arp/>
- Curman, A. S. N., Andresen, M. A., & Brantingham, P. J. (2015). Crime and Place: A Longitudinal Examination of Street Segment Patterns in Vancouver, BC. *Journal of Quantitative Criminology*, 31(1), 127–147. <https://doi.org/10.1007/s10940-014-9228-3>
- Daniels, J. A., Volungis, A., Pshenishny, E., Gandhi, P., Winkler, A., Cramer, D. P., & Bradley, M. C. (2010). A Qualitative Investigation of Averted School Shooting Rampages. *The Counseling Psychologist*, 38(1), 69–95. <https://doi.org/10.1177/0011000009344774>
- Davey, A. (2016). *Integrating crime prevention into urban design and planning*. <https://doi.org/10.1108/JPMD-09-2015-0043>
- Davey, C. L., & Wootton, A. B. (2016). Integrating crime prevention into urban design and planning: From European procedures to local delivery methods. In *Journal of Place Management and Development* (Vol. 9, Issue 2, pp. 153–165). Emerald Group Publishing Ltd. <https://doi.org/10.1108/JPMD-09-2015-0043>
- David, B. (2022). *Electric Vehicle Chargers Hacked to Show Porn*. Infosecurity Magazine. <https://www.infosecurity-magazine.com/news/electric-vehicle-chargers-hacked/>
- Davies, T., & Johnson, S. D. (2015). Examining the Relationship Between Road Structure and Burglary Risk Via Quantitative Network Analysis. *Journal of Quantitative Criminology*, 31(3), 481–507. <https://doi.org/10.1007/s10940-014-9235-4>
- Daws, R. (2023). *CISA urges manufacturers to end default passwords*. Telecoms. <https://www.telecomstechnews.com/news/cisa-urges-manufacturers-end-default-passwords/>
- DCMS-d. (2018). *Security of Network and Information Systems Guidance for Competent Authorities*.

- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701050/NIS_-_Guidance_for_Competent_Authorities.pdf
- DCMS. (2021, October 25). *Secure connected places (smart cities) guidance collection* - GOV.UK. <https://www.gov.uk/government/publications/secure-connected-places-smart-cities-guidance-collection>
- DCMS. (2022a, July 6). *Designing your connected place to be resilient* - GOV.UK. <https://www.gov.uk/government/publications/secure-connected-places-smart-cities-guidance-collection/designing-your-connected-place-to-be-resilient>
- DCMS. (2022b, November 3). *Secure connected places* - GOV.UK. <https://www.gov.uk/guidance/secure-connected-places>
- DCMS. (2023, January 4). *The NIS Regulations 2018* - GOV.UK. Gov.Uk. <https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018>
- De Souza, E., & Miller, J. (2012). HOMICIDE IN THE BRAZILIAN FAVELA: Does Opportunity Make the Killer? In *Source: The British Journal of Criminology* (Vol. 52, Issue 4).
- Deepaisarn, S., Yiwsiw, P., Chaisawat, S., Lerttomolsakul, T., Cheewakriengkrai, L., Tantiwattanapaibul, C., Buaruk, S., & Sornlertlamvanich, V. (2023). Automated Street Light Adjustment System on Campus with AI-Assisted Data Analytics. *Sensors*, 23(4). <https://doi.org/10.3390/s23041853>
- Demertzi, V., Demertzis, S., & Demertzis, K. (2023). An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. *Applied Sciences* 2023, Vol. 13, Page 790, 13(2), 790. <https://doi.org/10.3390/APP13020790>
- Deng, C. (2015). Integrating multi-source remotely sensed datasets to examine the impact of tree height and pattern information on crimes in Milwaukee, Wisconsin. *Applied Geography*, 65, 38–48. <https://doi.org/10.1016/j.apgeog.2015.10.005>
- Deng, M., Yang, W., Chen, C., & Liu, C. (2021). Exploring associations between streetscape factors and crime behaviors using Google Street View images. *Frontiers of Computer Science*, 16(4), 164316. <https://doi.org/10.1007/s11704-020-0007-z>
- Department for Business, E. & I. S. and T. R. H. G. C. M. (2018, November 22). *From science fiction to reality: People in London and Edinburgh set to be the first to trial self-driving vehicle services*. Gov.Uk. <https://www.gov.uk/government/news/from-science-fiction-to-reality-people-in-london-and-edinburgh-set-to-be-the-first-to-trial-self-driving-vehicle-services>
- Department for Business Energy & Industrial Strategy. (2021). Smart Meter Policy Framework Post 2020: Government Response to a Consultation on Minimum Annual Targets and Reporting Thresholds for Energy Suppliers. In *BEIS*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/990525/smart-meter-policy-framework-post-2020-govt-response-minimum-annual-targets.pdf
- Department for Transport. (2019a). *Electric Vehicle Smart Charging*.

- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/817107/electric-vehicle-smart-charging.pdf
- Department for Transport. (2019b). *Future of Mobility: Urban Strategy*. <https://assets.publishing.service.gov.uk/media/5dcd8417ed915d071ca239e9/future-of-mobility-strategy.pdf>
- Department for Transport. (2019c). *Future of mobility: urban strategy*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/846593/future-of-mobility-strategy.pdf
- Department for Transport. (2020). *A better deal for bus users*. Gov.Uk. <https://www.gov.uk/government/publications/a-better-deal-for-bus-users/a-better-deal-for-bus-users#summary-of-commitments>
- Department for Transport. (2021). *National Bus Strategy: Bus Service Improvement Plans*. <https://assets.publishing.service.gov.uk/media/609baca0e90e073576198c16/bus-service-improvement-plans-guidance-to-local-authorities-and-bus-operators.pdf>
- Department for Transport. (2022, January). *Electric vehicle charging device statistics - GOV.UK*. <https://www.gov.uk/government/statistics/electric-vehicle-charging-device-statistics-january-2022/electric-vehicle-charging-device-statistics-january-2022>
- DfT. (2007). *Manual for Streets*. https://assets.publishing.service.gov.uk/media/6270d4838fa8f57a360f8b91/Ess ex_Manual_for_Streets_Redacted.pdf
- DfT. (2019). *Updating Manual for Streets*. <https://www.ciht.org.uk/media/11568/manual-for-streets-webinar-sg.pdf>
- DfT. (2023). *Electric vehicle charging device statistics: July 2023*. Open Government Licence v3.0. <https://www.gov.uk/government/statistics/electric-vehicle-charging-device-statistics-july-2023>
- Díaz, C., Fossati, S., & Trajtenberg, N. (2022). Stay at home if you can: COVID-19 stay-at-home guidelines and local crime. *Journal of Empirical Legal Studies*, 19(4), 1067–1113. <https://doi.org/10.1111/jels.12336>
- Dimase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). *Systems engineering framework for cyber physical security and resilience*. <https://doi.org/10.1007/s10669-015-9540-y>
- Ding, N., Zhai, Y. ming, Hu, X. feng, & Ma, M. yuan. (2019). Crime prediction of bicycle theft based on online search data. *Advances in Intelligent Systems and Computing*, 891, 117–128. https://doi.org/10.1007/978-3-030-03766-6_13
- Dormehl. (2016, November 7). *The road to tomorrow: streets need to be as smart as the cars driving on them*. Wired UK. <https://www.wired.co.uk/article/smart-cars-need-smart-streets>
- Dowden, O. (2022). *Security Update on Surveillance Equipment*. UK Parliament. <https://questions-statements.parliament.uk/written-statements/detail/2022-11-24/hcws386>

- DSIT. (2019a). *Collection - Secure By Design*.
<https://www.gov.uk/government/collections/secure-by-design>
- DSIT. (2019b). *SECURE CONNECTED PLACES INCIDENT RESPONSE In collaboration with*.
- DSIT. (2022). *The Smart Street Infrastructure Security Report: executive summary*. Gov.Uk. <https://www.gov.uk/government/publications/the-smart-street-infrastructure-security-report/the-smart-street-infrastructure-security-report-executive-summary>
- DSIT. (2023, June). *Secure connected places playbook - GOV.UK*. DSIT. <https://www.gov.uk/guidance/secure-connected-places-playbook>
- DSIT. (2024a). *Cyber security breaches survey 2024*. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024>
- DSIT. (2024b). *Guidance: Governance in a box*. Secure Connected Places Playbook. <https://www.gov.uk/government/publications/secure-connected-places-playbook-documents/governance-in-a-box#:~:text=The use of the Governance,security of their connected places>
- Dunning, R., Calafiore, A., & Nurse, A. (2021). 20-minute neighbourhood or 15-minute city? *Town and Country Planning*. <https://www.rtpi.org.uk/find-your-rtpi/rtpi-english-regions/rtpi-london/latest-updates/15-minute-cities20-minute-neighbourhoods/#:~:text=The idea of 'fifteen minute,today's most popular planning paradigm>
- Durhamradionews. (2021). *Speed cameras in Durham issue thousands of tickets despite being targeted by vandals*. Durhamradionews.Com. <https://www.durhamradionews.com/archives/132742>
- e Oliveira, E., Miguéis, V. L., & Borges, J. L. (2022). Automatic root cause analysis in manufacturing: an overview & conceptualization. *Journal of Intelligent Manufacturing*, 1–18. <https://doi.org/10.1007/S10845-022-01914-3/TABLES/10>
- Eachus, P., Stedmon, A., & Baillie, L. (2013). Hostile intent in public crowded spaces: A field study. *Applied Ergonomics*, 44(5), 703–709. <https://doi.org/10.1016/J.APERGO.2012.05.009>
- Eakambaram, M. (2017). *Smart Street Lights for Brighter Savings and Opportunities*. Solution Brief, Intel. <https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/smart-street-lights-for-brighter-savings-solutionbrief.pdf>
- Eck, J. E. (2010). *Encyclopedia of Criminological Theory Places and the Crime Triangle*. <https://doi.org/10.4135/9781412959193.n77>
- Eck, J. E., Clarke, R. V., & Guerette, R. T. (2007). *Crime Prevention Studies* (Vol. 21).
- Eck, J. E., Clarke, R. V., Guerette, R. T., & others. (2007). Risky facilities: Crime concentration in homogeneous sets of establishments and facilities. *Crime Prevention Studies*, 21, 225. https://popcenter.asu.edu/sites/default/files/tools/risky_facilities/PDFs/Eck_et_al_press.pdf

- Eck, J. E., & Guerette, R. T. (2012). Place-based crime prevention: Theory, evidence, and policy. *The Oxford Handbook of Crime Prevention*, 354–383.
- Eck, J. E., & Weisburd, D. (1995). *CRIME PLACES IN CRIME THEORY*. Criminal Justice Press/Willow Tree Press. <http://www.ncjrs.gov/App/publications/abstract.aspx?ID=160731%0A>
- Eklom, P. (2011a). Deconstructing CPTED... and Reconstructing it for Practice, Knowledge Management and Research. *European Journal on Criminal Policy and Research*, 17(1), 7–28. <https://doi.org/10.1007/s10610-010-9132-9>
- Eklom, P. (2011b). Deconstructing CPTED... and Reconstructing it for Practice, Knowledge Management and Research. *European Journal on Criminal Policy and Research*, 17(1), 7–28. <https://doi.org/10.1007/s10610-010-9132-9>
- Eklom, P. (2017). *Crime, situational prevention and technology: The nature of opportunity and how it evolves* (1st ed., pp. 353–374). Routledge. <https://doi.org/10.4324/9781315743981-21>
- Eklom, P., & Pease, K. (2014). Innovation and crime prevention. *Encyclopedia of Criminology and Criminal Justice*. New York: Springer Science+ Business Media.
- Eken, S., & Sayar, A. (2014). A smart bus tracking system based on location-aware services and QR codes. *INISTA 2014 - IEEE International Symposium on Innovations in Intelligent Systems and Applications, Proceedings*, 299–303. <https://doi.org/10.1109/INISTA.2014.6873634>
- ElHussini, H., Assi, C., Moussa, B., Atallah, R., & Ghrayeb, A. (2021). A tale of two entities: Contextualizing the security of electric vehicle charging stations on the power grid. *ACM Transactions on Internet of Things*, 2(2), 1–21.
- Elmo, D., Fragkos, G., Johnson, J., Rohde, K., Salinas, S., & Zhang, J. (2023). Disrupting EV Charging Sessions and Gaining Remote Code Execution with DoS, MITM, and Code Injection Exploits using OCPP 1.6. *2023 Resilience Week (RWS)*, 1–8.
- Elsevier B.V. (2020a). *Ovid Database Guide*. <https://ospguides.ovid.com/OSPguides/elgedb.htm>
- Elsevier B.V. (2020b). *Scopus*. <https://www.scopus.com/sources.uri?zone=TopNavBar&origin=searchbasic>
- Energy Systems Catapult. (2020). *EV Energy Taskforce: The Road to Electric Vehicles*. Energising Our Electric Vehicle Transition- Moving from Proposal to Action. <https://es.catapult.org.uk/project/ev-energy-taskforce-the-road-to-electric-vehicles/>
- ENISA. (2017). *NIS Directive*. ENISA. <https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii/nis-directive>
- ENISA. (2024). *ENISA Good practices for IoT and Smart Infrastructures Tool*. 2005-2024 by the European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool>
- Epiphaniou, G., Hammoudeh, M., Yuan, H., Maple, C., & Ani, U. (2023). *Simulation*

- Modelling Practice and Theory* 125 (2023) 102744 Available online 15. 1569–190.
<https://doi.org/10.1016/j.simpat.2023.102744>
- Escalante, M., & Capstone, A. (2018). *ONION ROUTER TOR, BLOCKCHAIN TECHNOLOGY AND CYBERCRIMINALS*.
- ESRB. (2020). *Systemic cyber risk*. <https://doi.org/10.2849/566567>
- Euro Cities. (2021, September 30). *Managing urban traffic: 3D zebra crossings spread across Europe - Eurocities*. <https://eurocities.eu/stories/managing-urban-traffic-3d-zebra-crossings-spread-across-europe/>
- European Commission. (2023a). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
- European Commission. (2023b). *The EU Cyber Solidarity Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>
- Europol. (2015). Europol Press Release. <https://www.europol.europa.eu/newsroom/news/massive-changes-in-criminal-landscape>
- Europol. (2021). *INTERNET ORGANISED CRIME THREAT ASSESSMENT 2021*. https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf
- EV Energy Taskforce. (2023). *Drivers for Success 2035 -Electric Vehicle Energy Taskforce*. <https://evenergytaskforce.com/reports/ev-energy-taskforce-drivers-for-success-2035/>
- EV Energy Taskforce Working Group 3. (2021). *Cyber Security and Smart Charging*.
- Evans, J. M., & Kebbell, M. R. (2012). The effective analyst: a study of what makes an effective crime and intelligence analyst. *Policing and Society*, 22(2), 204–219. <https://doi.org/10.1080/10439463.2011.605130>
- Eveleth, R. (2016). *Facial recognition systems display inherent bias*. Motherboard. <https://privacyinternational.org/examples/1827/facial-recognition-systems-display-inherent-bias>
- Extrapolate. (2023, January 23). *Global Electric Vehicle Market and EV Charging Station*. <https://www.globenewswire.com/news-release/2023/01/23/2593238/0/en/Global-Electric-Vehicle-Market-and-EV-Charging-Station-Market-Size-Share-Revenue-Emerging-Technologies-Growing-Demand-Latest-Innovations-Industry-Updates-and-Future-Growth-Extrapol.html>
- Fang, E. H. C., & Kumar, S. (2019). The trends and challenges of 3D printing. *Advanced Methodologies and Technologies in Engineering and Environmental Science*, 415–423.
- Farrell, G., & Pease, K. (2006). Criminology and security. *The Handbook of Security*, 179–199.
- Farrell, G., & Pease, K. (Kenneth). (2010). *Repeat victimization / edited by Graham*

Farrell, Ken Pease. Boulder, Colo .

Farrington, D. P., & Welsh, B. C. (2002). Improved street lighting and crime prevention. *Justice Quarterly*, 19(2), 313–342. <https://doi.org/10.1080/07418820200095261>

Farrington David P., W. B. (2002). *Effects of improved street lighting on crime : a systematic review / David P. Farrington and Brandon C. Welsh. - University College London.* https://ucl-new-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=UCL_LMS_DS21132612980004761&context=L&vid=UCL_VU2&lang=en_US&search_scope=CSCOP_UCL&adaptor=Local Search Engine&tab=local&query=any,contains,crime on street&offset=0

Fatehkia, M., O'Brien, D., & Weber, I. (2019). Correlated impulses: Using Facebook interests to improve predictions of crime rates in urban areas. *PLoS ONE*, 14(2). <https://doi.org/10.1371/journal.pone.0211350>

Favarin, S. (2018). This must be the place (to commit a crime). Testing the law of crime concentration in Milan, Italy. *European Journal of Criminology*, 15(6), 702–729. <https://doi.org/10.1177/1477370818757700>

Ficco, M., Choraś, M., & Kozik, R. (2017). Simulation platform for cyber-security and vulnerability analysis of critical infrastructures. *Journal of Computational Science*, 22, 179–186. <https://doi.org/10.1016/J.JOCS.2017.03.025>

Fisher, D., Maimon, D., & Berenblum, T. (2022). Examining the crime prevention claims of crime prevention through environmental design on system-trespassing behaviors: a randomized experiment. *Security Journal*, 35(2), 400–422. <https://doi.org/10.1057/s41284-020-00282-y>

Forbes Home. (2024). *Internet Usage Statistics In 2024.* <https://www.forbes.com/home-improvement/internet/internet-statistics/>

Franceschi-Bicchierai, L. (2016, August 5). *Afraid of the Dark? Too Bad, Your Smart Bulbs Can Be Hacked.* Motherboard. <https://www.vice.com/en/article/d7yxxw/hackers-could-take-control-of-your-smart-light-bulbs-and-cause-a-blackout>

Frick, K. T., MENDONÇA, A. G., MALKIN, N., Pan, A., & Post, A. E. (2021). *The Cybersecurity Risks of Smart City Technologies.* https://cltc.berkeley.edu/wp-content/uploads/2021/03/Smart_City_Cybersecurity.pdf

Fridman, R. (2023, January 29). *The 9 top trends driving electric vehicle security in 2023 - ISRAEL21c.* ISRAEL21c. <https://www.israel21c.org/the-9-top-trends-driving-electric-vehicle-security-in-2023/>

Friedman, L. (2001). Why vote-count reviews don't count (multiple letters). In *Biological Psychiatry* (Vol. 49, Issue 2, pp. 161–162). Elsevier. [https://doi.org/10.1016/S0006-3223\(00\)01075-1](https://doi.org/10.1016/S0006-3223(00)01075-1)

Frith, M. J., Johnson, S. D., & Fry, H. M. (2017). ROLE OF THE STREET NETWORK IN BURGLARS' SPATIAL DECISION-MAKING*. *Criminology*, 55(2), 344–376. <https://doi.org/10.1111/1745-9125.12133>

Fruhlinger, J. (2018). *The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet.* CSO. <https://www.csoonline.com/article/564711/the-mirai-botnet-explained-how-teen->

scammers-and-cctv-cameras-almost-brought-down-the-internet.html

- Furfaro, A., Felicetti, C., Saccà, D., & Crupi, F. (2023). *Accountability of IoT Devices BT - Security, Trust and Privacy Models, and Architectures in IoT Environments* (L. Fotia, F. Messina, D. Rosaci, & G. M. L. Sarné (Eds.); pp. 133–147). Springer International Publishing. https://doi.org/10.1007/978-3-031-21940-5_8
- Galle, N. J., Nitoslowski, S. A., & Pilla, F. (2019). The Internet of Nature: How taking nature online can shape urban ecosystems. *The Anthropocene Review*, 6(3), 279–287. <https://doi.org/10.1177/2053019619877103>
- Garcia-Font, V., Garrigues, C., & Rifà-Pous, H. (2016). *A Comparative Study of Anomaly Detection Techniques for Smart City Wireless Sensor Networks*. <https://doi.org/10.3390/s16060868>
- Garofalaki, Z., Kosmanos, D., Moschoyiannis, S., Kallergis, D., & Douligeris, C. (2022). Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (OCPP). *IEEE Communications Surveys & Tutorials*, 24(3), 1504–1533.
- Gavrovska, A., & Samčović, A. (2020). Intelligent Automation Using Machine and Deep Learning in Cybersecurity of Industrial IoT: CCTV Security and DDoS Attack Detection. In *Cyber Security of Industrial Control Systems in the Future Internet Environment* (pp. 156–174). IGI Global.
- Gear, L. (2021). *Thermal Management for Electric Vehicles 2021-2031 Copyright , Use and Disclaimer*. <https://www.idtechex.com/en/research-report/thermal-management-for-electric-vehicles-2021-2031/822>
- Gerell, M. (2016). Hot Spot Policing With Actively Monitored CCTV Cameras. *International Criminal Justice Review*, 26(2), 187–201. <https://doi.org/10.1177/1057567716639098>
- Ghafouri, M., Kabir, E., Moussa, B., & Assi, C. (2022). Coordinated charging and discharging of electric vehicles: A new class of switching attacks. *ACM Transactions on Cyber-Physical Systems (TCPS)*, 6(3), 1–26.
- Ghappour, A., Calo, R., Chander, A., Chesney, B., Citron, D., Daskal, J., Dodge, B., Dodson, S., Jinks, D., Joh, E., Kerr, O., Marcus, R., Mikkilineni, T., Ohm, P., Parrish, A., Pell, S. K., Ratner, M., Ross, B., Schiller, R., ... Strandburg, K. (2017). *Stanford Law Review Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*. <https://poseidon01.ssrn.com/delivery.php?ID=2031110700870690150071031050970670750150440570060320320650301270760130660810040250280020590371270430630281060720981061130840281030230400330281251060930801270240720950030790140221190220051071270740051110290101010>
- Gianluca, M. (2016). *Could Britain's "smart cities" be outsmarted by cyber hackers?* Mashable. <https://mashable.com/article/smart-cities-ddos-attacks>
- Gibson, V., & Johnson, D. (2016). CPTED, but not as we know it: Investigating the conflict of frameworks and terminology in crime prevention through environmental design. *Security Journal*, 29(2), 256–275. <https://doi.org/10.1057/sj.2013.19>
- Girdhar, M., Hong, J., Lee, H., & Song, T.-J. (2021). Hidden markov models-based

- anomaly correlations for the cyber-physical security of ev charging stations. *IEEE Transactions on Smart Grid*, 13(5), 3903–3914.
- Girdhar, M., Hong, J., Yoo, Y., & Song, T. (2022). Machine learning-enabled cyber attack prediction and mitigation for ev charging stations. *2022 IEEE Power & Energy Society General Meeting (PESGM)*, 1–5.
- GLA. (2020). *Smart Street Infrastructure: Strategic assets for a true Smart City*. Sharing Cities. https://sharingcities.eu/wp-content/uploads/sites/6/2022/11/Sharing-Cities_Infrastructure-Playbook_VFfinal3-min.pdf
- Global, V. (2023). *SMART CHARGING OF ELECTRIC VEHICLES*. Virta. <https://www.virta.global/smart-charging>
- Goh, J., Kang, H., Koh, Z., Lim, J., Ng, C., Sher, G., & Yao, C. (2020). Cyber Risk Surveillance: A Case Study of Singapore. *IMF Working Papers*, 20. <https://doi.org/10.5089/9781513526317.001>
- Goode, S. D., & Goode, S. D. (2011). Encountering Paedophiles on the Internet. *Paedophiles in Society: Reflecting on Sexuality, Abuse and Hope*, 22–53.
- Gordon, F. (2022, July 26). *How big is the risk that someone will hack an EV charging network?* | *Ars Technica*. Ars Technica. <https://arstechnica.com/cars/2022/07/ev-charging-networks-create-a-tempting-target-for-cyberattacks/>
- Gorman, D. M., Speer, P. W., Gruenewald, P. J., & Labouvie, E. W. (2001). Spatial dynamics of alcohol availability, neighborhood structure and violent crime. *Journal of Studies on Alcohol*, 62(5), 628–636. <https://doi.org/10.15288/jsa.2001.62.628>
- Gov.uk. (2022). *Response to Consumer Market Authority investigation into Electric Vehicle Charging*. https://assets.publishing.service.gov.uk/media/6038ed30e90e070566dafa57/London_Councils__GLA__TfL__LGTAG.pdf
- Gov.UK. (2022, December 19). *The UK Government Resilience Framework (HTML)*. <https://www.gov.uk/government/publications/the-uk-government-resilience-framework/the-uk-government-resilience-framework-html>
- GOV.UK. (2023a). *Regulations: electric vehicle smart charge points*. Open Government Licence v3.0. <https://www.gov.uk/guidance/regulations-electric-vehicle-smart-charge-points>
- GOV.UK. (2023b, February 1). *UK Government backing helps launch world first self-driving bus*. <https://www.gov.uk/government/news/uk-government-backing-helps-launch-world-first-self-driving-bus>
- Government-a, H. M. (2017). *Secure by Design*. <https://www.security.gov.uk/policy-and-guidance/secure-by-design/>
- Gracias, J. S., Parnell, G. S., Specking, E., Pohl, E. A., & Buchanan, R. (2023). Smart Cities—A Structured Literature Review. In *Smart Cities* (Vol. 6, Issue 4, pp. 1719–1743). <https://doi.org/10.3390/smartcities6040080>
- Greater London Authority. (2016). *SMART LONDON PLAN Using the creative power of new technologies to serve London and improve Londoners' lives*.

https://www.london.gov.uk/sites/default/files/smart_london_plan.pdf

- Greater London Authority. (2020). *London City Resilience Strategy 2020*. https://www.london.gov.uk/sites/default/files/london_city_resilience_strategy_2020_digital.pdf
- Green, L. (1995). Cleaning up drug hot spots in oakland, california: The displacement and diffusion effects. *Justice Quarterly*, 12(4), 737–754. <https://doi.org/10.1080/07418829500096271>
- Groff, E., & Mccord, E. S. (2012). The role of neighborhood parks as crime generators. *Security Journal*, 25, 1–24. <https://doi.org/10.1057/sj.2011.1>
- Groff, E R, & McCord, E. S. (2011). The role of neighborhood parks as crime generators. *Secur J*, 25. <https://doi.org/10.1057/sj.2011.1>
- Groff, Elizabeth R., & Lockwood, B. (2014). Criminogenic Facilities and Crime across Street Segments in Philadelphia. *Journal of Research in Crime and Delinquency*, 51(3), 277–314. <https://doi.org/10.1177/0022427813512494>
- Groff, Elizabeth R., Weisburd, D., & Yang, S.-M. (2010). Is it Important to Examine Crime Trends at a Local “Micro” Level?: A Longitudinal Analysis of Street to Street Variability in Crime Trajectories. *Source: Journal of Quantitative Criminology*, 26(1), 7–32. <https://doi.org/10.1007/sl>
- Groff, Elizabeth R. (2014). Quantifying the Exposure of Street Segments to Drinking Places Nearby. *Source: Journal of Quantitative Criminology*, 30(3), 527–548. <https://doi.org/10.1007/s>
- Groff, Elizabeth R, & Lockwood, B. (2014). Criminogenic Facilities and Crime across Street Segments in Philadelphia: Uncovering Evidence about the Spatial Extent of Facility Influence. *Journal of Research in Crime and Delinquency*, 51(3), 277–314. <https://doi.org/10.1177/0022427813512494>
- Groff, Elizabeth R, & Mccord, E. S. (2012). The role of neighborhood parks as crime generators. *Security Journal*, 25, 1–24. <https://doi.org/10.1057/sj.2011.1>
- Grubestic, T. H., & Pridemore, W. A. (2011). *Alcohol outlets and clusters of violence*. <https://doi.org/10.1186/1476-072X-10-30>
- Guerette, R. T., & Bowers, K. J. (2009). ASSESSING THE EXTENT OF CRIME DISPLACEMENT AND DIFFUSION OF BENEFITS: A REVIEW OF SITUATIONAL CRIME PREVENTION EVALUATIONS. *Criminology (Beverly Hills)*, 47(4), 1331–1368. <https://doi.org/10.1111/j.1745-9125.2009.00177.x>
- Guerette, R. T., & Clarke, R. V. (2003). Product Life Cycles and Crime: Automated Teller Machines and Robbery. *Security Journal*, 16(1), 7–18. <https://doi.org/10.1057/palgrave.sj.8340122>
- Guerrero-Ibáñez, J., Zeadally, S., & Contreras-Castillo, J. (2018). Sensor Technologies for Intelligent Transportation Systems. *Sensors*, 18(4), 1212. <https://doi.org/10.3390/S18041212>
- Gumrukcu, E., Arsalan, A., Muriithi, G., Joglekar, C., Aboulebddeh, A., Zehir, M. A., Papari, B., & Monti, A. (2022). Impact of Cyber-attacks on EV Charging Coordination: The Case of Single Point of Failure. *2022 4th Global Power, Energy*

- and Communication Conference (GPECOM), 506–511.
<https://doi.org/10.1109/GPECOM55404.2022.9815727>
- Gupta, B. B., Nalin, ., Arachchilage, A. G., Psannis, K. E., Gupta, B. B. B., Arachchilage, N. A. G., & Gr, K. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, 67, 247–267. <https://doi.org/10.1007/s11235-017-0334-z>
- H.M.Government. (2016). *National Cyber Security Strategy 2016-2021*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
- H M Government. (2017). *The key principles of vehicle cyber security for connected and automated vehicles* - GOV.UK. <https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles>
- Haberman, C. P., & Kelsay, J. D. (2021). The Topography of Robbery: Does Slope Matter? *Journal of Quantitative Criminology*, 37(3), 625–645. <https://doi.org/10.1007/s10940-020-09451-z>
- Haberman, C. P., & Ratcliffe, J. H. (2015). Testing for Temporally Differentiated Relationships among Potentially Criminogenic Places and Census Block Street Robbery Counts. *Criminology*, 53. <https://heinonline.org/HOL/Page?handle=hein.journals/crim53&id=479&div=29&collection=journals>
- Haberman, C. P., Sorg, E. T., & Ratcliffe, J. H. (2017). Assessing the Validity of the Law of Crime Concentration Across Different Temporal Scales. *Journal of Quantitative Criminology*, 33, 547–567. <https://doi.org/10.1007/s10940-016-9327-4>
- Hackread. (2017, February 2). *Two Arrested in UK for Hacking DC CCTV Cameras Before Trump Inauguration*. <https://www.hackread.com/hackers-arrested-for-hacking-cctv-cameras/>
- Hamdare, S., Kaiwartya, O., Aljaidi, M., Jugran, M., Cao, Y., Kumar, S., Mahmud, M., Brown, D., & Lloret, J. (2023). Cybersecurity risk analysis of electric vehicles charging stations. *Sensors*, 23(15), 6716.
- Hammi, B., Khatoun, R., Zeadally, S., Fayad, A., & Khoukhi, L. (2018). IoT technologies for smart cities. *IET Networks*, 7(1), 1–13. <https://doi.org/10.1049/IET-NET.2017.0163>
- Hammond, B. (2012). ENISA RECOMMENDS COOPERATION AMONG CERTs, LAW ENFORCEMENT ON CYBER CRIME. *Cybersecurity Policy Report*. https://search-proquest-com.libproxy.ucl.ac.uk/docview/950856172?rfr_id=info%3Axri%2Fsid%3Aprimo
- Harmony, X. J., & Gayah, V. V. (2017). Evaluation of Real-Time Transit Information Systems: An information demand and supply approach. *International Journal of Transportation Science and Technology*, 6(1), 86–98. <https://doi.org/https://doi.org/10.1016/j.ijtst.2017.05.003>

- Harnett, K., Harris, B., Chin, D., Watson, G., & others. (2018). *Doe/dhs/dot volpe technical meeting on electric vehicle and charging station cybersecurity report*. <https://rosap.ntl.bts.gov/view/dot/34991>
- Hart, T. C., & Miethe, T. D. (2015). Configural Behavior Settings of Crime Event Locations. *Journal of Research in Crime and Delinquency*, 52(3), 373–402. <https://doi.org/10.1177/0022427814566639>
- Hassen, N., & Kaufman, P. (2016). Examining the role of urban street design in enhancing community engagement: A literature review. *Health & Place*, 41, 119–132. <https://doi.org/10.1016/j.healthplace.2016.08.005>
- Havlin, S., Araujo, N. A. M., Buldyrev, S. V, Dias, C. S., Parshani, R., Paul, G., & Stanley, H. E. (2010). Catastrophic Cascade of Failures in Interdependent Networks. In *arXiv.org*. <https://www.proquest.com/working-papers/catastrophic-cascade-failures-interdependent/docview/2087612267/se-2?accountid=14511>
- He, L., Liu, S., & Shen, Z. M. (2022). Smart urban transport and logistics: A business analytics perspective [Article]. *Production and Operations Management*, 31(10), 3771–3787. <https://doi.org/10.1111/poms.13775>
- Heidari, Arash, Nima Jafari Navimipour, Mehmet Unal, G. Z. (2023). Machine Learning Applications in Internet-of-Drones: Systematic Review, Recent Deployments, and Open Issues. *ACM Computing Surveys*, 55(12). <https://doi.org/10.1145/3571728>
- Heidari, A., Jafari Navimipour, N., Unal, M., & Zhang, G. (2023). Machine Learning Applications in Internet-of-Drones: Systematic Review, Recent Deployments, and Open Issues. *ACM Computing Surveys*, 55(12), 1–45. <https://doi.org/10.1145/3571728>
- Helfenstein, U. (2002). Data and models determine treatment proposals - An illustration from meta-analysis. In *Postgraduate Medical Journal* (Vol. 78, Issue 917, pp. 131–134). <https://doi.org/10.1136/pmj.78.917.131>
- Herrera, L.-C., & Maennel, O. (2019). A comprehensive instrument for identifying critical information infrastructure services. *International Journal of Critical Infrastructure Protection*, 25, 50–61. <https://doi.org/10.1016/j.ijcip.2019.02.001>
- Herrmann, C. R. (2015). The dynamics of robbery and violence hot spots. *Crime Science*, 4(1), 1–14. <https://doi.org/10.1186/s40163-015-0042-5>
- Higgins, J. P. T., Thomas, J., Chandler, J., Cumpston, M., Li, T., Page, M. J., & Welch, V. A. (Eds.). (2019). *Cochrane Handbook for Systematic Reviews of Interventions*. Wiley. <https://doi.org/10.1002/9781119536604>
- Hill, K. (2020). Facial Match And Arrest Go Wrong [Article]. *The New York Times*, B1.
- Hill, M. (2022, March 8). *London UK's most attacked region, over 5,000 cybercrimes reported in 2021*. CSO Online. <https://www.csoonline.com/article/3652534/london-uk-s-most-attacked-region-over-5-000-cybercrimes-reported-in-2021.html>
- Hinduja, S., & Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal*, 26(4), 383–402. <https://doi.org/10.1057/sj.2013.25>

- Hino, K. (2022). Changes in public attitudes toward CCTV installations in residential areas between 2008 and 2019. *Cities*, 128, 103810. <https://doi.org/10.1016/J.CITIES.2022.103810>
- Hirschfield, A., Johnson, A., Bowers, S. D., Kate J., & Sheffield. (2001). *Review of major policy developments and evidence base: crime domain Original Citation Review of major policy developments and evidence base: crime domain. Project Report.*
- HM Government. (2022). *Taking charge: the electric vehicle infrastructure strategy.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1065576/taking-charge-the-electric-vehicle-infrastructure-strategy.pdf
- Ho, H., Ko, R., & Mazerolle, L. (2022). Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review. *Computers & Security*, 115, 102611. <https://doi.org/10.1016/j.cose.2022.102611>
- Hodge Cabell, Bennett Jesse, Bentley Julian, & Boyce Leidy. (2022). *Considerations for Department of Defense Implementation of ZeroEmission Vehicles and Charging Infrastructure.* <https://www.nrel.gov/docs/fy22osti/81925.pdf>
- Holland, S. P., Mansur, E. T., & Yates, A. J. (2021). The electric vehicle transition and the economics of banning gasoline vehicles. *American Economic Journal: Economic Policy*, 13(3), 316–344.
- Hollis-Peel, M. E., Reynald, D. M., van Bavel, M., Elffers, H., & Welsh, B. C. (2011). Guardianship for crime prevention: a critical review of the literature. *Crime, Law, and Social Change*, 56(1), 53–70. <https://doi.org/10.1007/s10611-011-9309-2>
- Holt, T. J., van Wilsem, J., van de Weijer, S., & Leukfeldt, R. (2020). Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review*, 38(2), 187–206.
- House of Commons. (2023). *National Security Act 2023.* UK Parliament. <https://bills.parliament.uk/bills/3154>
- Howell, C. J., Cochran, J. K., Powers, R. A., Maimon, D., & Jones, H. M. (2017). System trespasser behavior after exposure to warning messages at a Chinese computer network: An examination. *International Journal of Cyber Criminology*, 11(1), 63–77. <https://doi.org/10.5281/zenodo.495772>
- Hsieh, M. L., & Wang, S. Y. K. (2018). Routine activities in a virtual space: A Taiwanese case of an ATM hacking spree. *International Journal of Cyber Criminology*, 12(1), 333–352. <https://doi.org/10.5281/zenodo.1467935>
- Hsu, K.-H., & Miller, J. (2017). Assessing the Situational Predictors of Drug Markets across Street Segments and Intersections. *Journal of Research in Crime and Delinquency*, 54(6), 902–929. <https://doi.org/10.1177/0022427817714574>
- Huang, K., Siegel, M., & Madnick, S. (2017). *Cybercrime-as-a-Service: Identifying Control Points to Disrupt.* 1(1). <https://ic3.mit.edu/wp-content/uploads/2017/11/2017-17.pdf>
- Hudson-Smith, A., Wilson, D., Gray, S., & Dawkins, O. (2021). Urban IoT: Advances, Challenges, and Opportunities for Mass Data Collection, Analysis, and

- Visualization. *Urban Book Series*, 701–719. https://doi.org/10.1007/978-981-15-8983-6_38/FIGURES/6
- Hundal, R., Kowalyk, S., Wakim, A., Nikkel, C., Sink, J. H., & Doyle, M. (2020). Multicenter real-world assessment of the effectiveness of v-go wearable insulin delivery device in adult patients with type 2 diabetes (Enable study): A retrospective analysis. *Medical Devices (Auckland, N.Z.)*, 13, 283–291.
- Hunn, N. (2018). *How to Hack a Smart Meter and Kill the Grid – Creative Connectivity*. Creative Connectivity. <https://www.nickhunn.com/how-to-hack-a-smart-meter-and-kill-the-grid/>
- Hunt, S. C., & Young, N. L. (2021). Blending Indigenous Sharing Circle and Western Focus Group Methodologies for the Study of Indigenous Children's Health: A Systematic Review [Article]. *International Journal of Qualitative Methods*, 20, 160940692110151. <https://doi.org/10.1177/16094069211015112>
- Hussain, A. (2016). *Engineer gets 8 months' jail for hacking into police CCTV cameras at SEA Games 2015*. The Straitstimes. <https://www.straitstimes.com/singapore/courts-crime/engineer-gets-8-months-jail-for-hacking-into-police-cctv-cameras-at-sea-games#:~:text=Home-,Engineer gets 8 months' jail for hacking into police,cameras at SEA Games 2015&text=SINGAPORE - Just hours befo>
- Hyde, R. (2014). *The sci-fi future of lamp-posts*. The Guradian. <https://www.theguardian.com/cities/2014/nov/13/sci-fi-future-lamp-posts-street-lighting>
- ICO. (n.d.). *Drones* | ICO. Retrieved March 16, 2020, from <https://ico.org.uk/your-data-matters/drones/>
- ICO. (2014). *Governance (post-deployment)*. Guidance on Video Surveillance (Including CCTV). <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/governance-post-deployment/>
- IESE Insight. (2022, October 27). *London is the world's "smartest" city, according to IESE's Cities in Motion Index*. IESE. <https://www.iese.edu/insight/articles/london-worlds-smartest-city/>
- Illegal use of 3D printing* | PoliceOne.com. (n.d.). Retrieved February 28, 2019, from <https://www.policeone.com/police-products/3D-Laser-Scanners/articles/418682006-How-criminals-are-using-3D-printing/>
- Information Commissioner's Office. (2018). *Video surveillance (including guidance for organisations using CCTV)*. ICO. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/>
- Integrated Security*. (2014). [https://www.cpni.gov.uk/system/files/documents/40/20/Integrated Security Guide.pdf](https://www.cpni.gov.uk/system/files/documents/40/20/Integrated%20Security%20Guide.pdf)
- Intelligent Transport. (2021a). *Innovative, smart bus shelters to be introduced in Worcester, UK*. Intelligent Transport News.

- <https://www.intelligenttransport.com/transport-news/128702/smart-bus-shelters-worcester-uk/>
- Intelligent Transport. (2021b, October 15). *Bird trials new “Smart Sidewalk Protection” technology*. <https://www.intelligenttransport.com/transport-news/129137/bird-smart-sidewalk-protection-technology/>
- IoTNow. (2022, June 6). *EVs are great! But who’s keeping tabs on fraud risk at charging stations? | IoT Now News & Reports*. <https://www.iot-now.com/2022/06/06/121677-evs-are-great-but-whos-keeping-tabs-on-fraud-risk-at-charging-stations/>
- Irshad, M., Zhou, X., Noman, S. M., Murthy, A., Hu, B., Haider, S. A., & Olawale, O. A. (2021). City Vision: CCTV Images Based Public Surveillance Model. *2021 International Conference on Electronic Information Technology and Smart Agriculture (ICEITSA)*, 416–420. <https://doi.org/10.1109/ICEITSA54226.2021.00085>
- Irvin-Erickson, Y. (2015). *Identifying Risky Places for Crime: An Analysis of the Criminogenic Spatiotemporal Influences of Landscape Features on Street Robberies*. <https://www.ncjrs.gov/pdffiles1/nij/grants/248636.pdf>
- Ithaka. (2020). *JSTOR*. <https://about.jstor.org/>
- Jacobs, J. (2000). *The death and life of great American cities / Jane Jacobs*. London : Pimlico.
- Jacobs, J. B., & Haberman, A. (2017). 3D-printed firearms, do-it-yourself guns, \& the Second Amendment. *Law and Contemporary Problems*, 80(2), 129–147.
- Jacobs Karrie. (2022, June 29). *Toronto wants to kill the smart city forever | MIT Technology Review*. <https://www.technologyreview.com/2022/06/29/1054005/toronto-kill-the-smart-city/>
- James Black. (2018). *Self Driving Cars “Game Changing” for FBI...& ISIS*. The Cipher Brief. <https://www.thecipherbrief.com/article/exclusive/international/self-driving-cars-game-changing-fbi-isis>
- Jeffay, J. (2022). *Why Hackers Are Now Targeting Electric Car Charging Stations*. Nocamels - Israeli Innovation News. <https://nocamels.com/2022/08/why-hackers-are-now-targeting-electric-car-charging-stations/>
- Jeffery, C. R. (1969). Crime Prevention and Control Through Environmental Engineering. *Criminology*, 7(3), 35–58. <https://doi.org/10.1111/j.1745-9125.1969.tb00236.x>
- Jeffery, C. R. (1971). *Crime Prevention Through Environmental Design*.
- Jennings, J. M., Milam, A. J., Greiner, A., Furr- Holden, C. D. M., Curriero, F. C., & Thornton, R. J. (2014). Neighborhood alcohol outlets and the association with violent crime in one mid-Atlantic City: The implications for zoning policy. *Journal of Urban Health*, 91(1), 62–71. <https://doi.org/10.1007/s11524-013-9821-z>
- Jili, B. (2022). China’s surveillance ecosystem and the global spread of its tools. *Atlantic Council*, 17.

- Jin, D., Hannon, C., Li, Z., Cortes, P., Ramaraju, S., Burgess, P., Buch, N., & Shahidehpour, M. (2016). Smart street lighting system: A platform for innovative smart city applications and a new frontier for cyber-security [Article]. *The Electricity Journal*, 29(10), 28–35. <https://doi.org/10.1016/j.tej.2016.11.011>
- Joh, E. E. (2019). Policing the smart city. *International Journal of Law in Context*, 15(2), 177–182. <https://doi.org/DOI: 10.1017/S1744552319000107>
- Johnson, D., Gibson, V., & McCabe, M. (2014). Designing in crime prevention, designing out ambiguity: Practice issues with the CPTED knowledge framework available to professionals in the field and its potentially ambiguous nature. *Crime Prevention and Community Safety*, 16(3), 147–168. <https://doi.org/10.1057/cpcs.2014.3>
- Johnson, J., Anderson, B., Wright, B., Quiroz, J., Berg, T., Graves, R., Daley, J., Phan, K., Kunz, M., Pratt, R., & others. (2022). *Cybersecurity for electric vehicle charging infrastructure*.
- Johnson, J., Berg, T., Anderson, B., & Wright, B. (2022). Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses. *Energies* 2022, Vol. 15, Page 3931, 15(11), 3931. <https://doi.org/10.3390/EN15113931>
- Johnson, S. D., & Bowers, K. J. (2010). Permeability and Burglary Risk: Are Cul-de-Sacs Safer? *Journal of Quantitative Criminology*, 26(1), 89–111. <https://doi.org/10.1007/s10940-009-9084-8>
- Johnson, S. D., Guerette, R. T., Bowers, K., Johnson, S. D., Bowers, K., & Guerette, R. T. (2014). Crime displacement: what we know, what we don't know, and what it means for crime reduction. *J Exp Criminol*, 10, 5–5. <https://doi.org/10.1007/s11292-014-9209-4>
- Jones, D., Snider, C., Nassehi, A., Yon, J., & Hicks, B. (2020). Characterising the Digital Twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology*, 29, 36–52. <https://doi.org/10.1016/J.CIRPJ.2020.02.002>
- Jongejan, A., & Woldendorp, T. (1978). A Successful CPTED Approach: The Dutch “Police Label Secure Housing” on JSTOR. *JSTOR*, 39(1), 31–48. <https://www.jstor.org/stable/43296831>
- Joo, M., Seo, J., Oh, J., Park, M., & Lee, K. (2018). Situational Awareness Framework for Cyber Crime Prevention Model in Cyber Physical System. *International Conference on Ubiquitous and Future Networks, ICUFN, 2018-July*, 837–842. <https://doi.org/10.1109/ICUFN.2018.8436591>
- Jung, Y., & Yoon, Y. (2015). Behavior tracking model in dynamic situation using the risk ratio EM [Proceeding]. *2015 International Conference on Information Networking (ICOIN)*, 2015-, 444–448. <https://doi.org/10.1109/ICOIN.2015.7057942>
- Kabir, M. E., Ghafouri, M., Moussa, B., & Assi, C. (2021). A two-stage protection method for detection and mitigation of coordinated EVSE switching attacks. *IEEE Transactions on Smart Grid*, 12(5), 4377–4388.
- Kaffenberger, L., & Kopp, E. (2019). *Cyber Risk Scenarios, the Financial System, and*

- Systemic Risk Assessment*. Carnegie Endowment for International Peace. <https://carnegieendowment.org/2019/09/30/cyber-risk-scenarios-financial-system-and-systemic-risk-assessment-pub-79911>
- Kamal, M., Atif, M., Mujahid, H., Shanableh, T., Al-Ali, A. R., & Al Nabulsi, A. (2019). IoT Based Smart Bus Stops. *2019 3rd International Conference on Smart Grid and Smart Cities (ICSGSC)*, 6–9. <https://doi.org/10.1109/ICSGSC.2019.00-27>
- Karadimas, D., Papalambrou, A., Gialelis, J., & Koubias, S. (2016). An integrated node for Smart-City applications based on active RFID tags; Use case on waste-bins. *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2016-, 1–7.
- Kashef, M., Visvizi, A., & Troisi, O. (2021). Smart city as a smart service system: Human-computer interaction and smart city surveillance systems. *ScienceDirect*, 124(106923). <https://doi.org/10.1016/j.chb.2021.106923>
- Katsarov, M. (2023). *The Intersection Of Data Security And Smart Public Transit Systems*. Forbes. <https://www.forbes.com/sites/forbestechcouncil/2023/03/21/the-intersection-of-data-security-and-smart-public-transit-systems/>
- Kavak, H., Padilla, J. J., Vernon-Bido, D., Gore, R., & Diallo, S. (2016). A characterization of cybersecurity simulation scenarios. *SpringSim (CNS)*, 3.
- Khan, O. G. M., El-Saadany, E., Youssef, A., & Shaaban, M. (2021). Impact of Electric Vehicles Botnets on the Power Grid. *ArXiv.Org*. <https://doi.org/10.48550/arxiv.2103.09153>
- Khan, P. W., Byun, Y.-C., & Park, N. (2020). A data verification system for cctv surveillance cameras using blockchain technology in smart cities [Article]. *Electronics (Basel)*, 9(3), 484. <https://doi.org/10.3390/electronics9030484>
- Khatoun, R., & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine*, 55(3), 51–59. <https://doi.org/10.1109/MCOM.2017.1600297CM>
- Khey, D. N., & Sainato, V. A. (2013). Examining the correlates and spatial distribution of organizational data breaches in the United States. *Security Journal*, 26(4), 367–382. <https://doi.org/10.1057/sj.2013.24>
- Kim, J., Lee, D., & Park, N. (2020). CCTV-RFID enabled multifactor authentication model for secure differential level video access control [Article]. *Multimedia Tools and Applications*, 79(31–32), 23461–23481. <https://doi.org/10.1007/s11042-020-09016-z>
- Kim, Seungil, Kim, D., & Jung, S. (2017). Analysis of the Effect of Cul-de-sacs' Permeability Factors in Low-Rise Residential Areas on Burglary. *Journal of Asian Architecture and Building Engineering*, 16(3), 487–493. <https://doi.org/10.3130/jaabe.16.487>
- Kim, Sungyop, Ulfarsson, G. F., & Todd Hennessy, J. (2007). Analysis of light rail rider travel behavior: Impacts of individual, built environment, and crime characteristics on transit access. *Transportation Research Part A: Policy and Practice*, 41(6), 511–522. <https://doi.org/10.1016/J.TRA.2006.11.001>

- Kim, Y.-A., & Wo, J. C. (2022). Seasonality and Crime in Orlando Neighbourhoods. *British Journal of Criminology*, 62(1), 124–144. <https://doi.org/10.1093/bjc/azab048>
- Kim, Y.-A., & Wo, J. C. (2023). Topography and crime in place: The effects of elevation, slope, and betweenness in San Francisco street segments. *Journal of Urban Affairs*, 45(6), 1120–1144. <https://doi.org/10.1080/07352166.2021.1901591>
- Kim, Y. A., & Hipp, J. R. (2019). Pathways: Examining Street Network Configurations, Structural Characteristics and Spatial Crime Patterns in Street Segments. *Journal of Quantitative Criminology*, 1–28. <https://doi.org/10.1007/s10940-019-09428-7>
- Kingson, J. A. (2021). *The future of “smart” cities is in streetlights*. Axios. <https://www.axios.com/2021/02/11/smart-cities-street-lights>
- Kinney, J. B., Brantingham, P. L., Wuschke, K., Kirk, M. G., & Brantingham, P. J. (1978). Crime Attractors, Generators and Detractors: Land Use and Urban Crime Opportunities. In *Environment* (Vol. 34, Issue 1). <https://about.jstor.org/terms>
- Kinney, J. B., Brantingham, P. L., Wuschke, K., Kirk, M. G., & Brantingham, P. J. (2008). Crime attractors, generators and detractors: Land use and urban crime opportunities. *Built Environment*, 34(1), 62–74. <https://doi.org/10.2148/benv.34.1.62>
- Kitchin, R., & Dodge, M. (2019). The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention [Article]. *The Journal of Urban Technology*, 26(2), 47–65. <https://doi.org/10.1080/10630732.2017.1408002>
- Knapp, J. (2013). Safety and urban design – the role of CPTED in the design process. *Safer Communities*, 12(4), 176–184. <https://doi.org/10.1108/SC-07-2013-0015>
- Kobie, N. (2015). *Why smart cities need to get wise to security – and fast*. Guardian. <https://www.theguardian.com/technology/2015/may/13/smart-cities-internet-things-security-cesar-cerrudo-ioactive-labs>
- Köhler, S., Baker, R., Strohmeier, M., & Martinovic, I. (2022). End-to-End Wireless Disruption of CCS EV Charging. *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 3515–3517.
- Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets [Article]. *Computer (Long Beach, Calif.)*, 50(7), 80–84. <https://doi.org/10.1109/MC.2017.201>
- Kollewe, J. (2021, November 9). *Thousands of UK phone boxes to be protected from closure | BT*. The Guardian. <https://www.theguardian.com/business/2021/nov/09/uk-phone-boxes-bt-poor-mobile-coverage>
- Kulinskaya, E., Morgenthaler, S., & Staudte, R. G. (2007). *Meta Analysis*. John Wiley & Sons, Ltd. <https://doi.org/10.1002/9780470985533>
- Kumar, B. V., Ravishankar, A., Karan, A., Vishal, K., & Praseeth Kumar, J. A. (2020). A smart public transportation system for reliable and hassle free conveyance in sustainable smart cities. *2020 International Conference on Computer Communication and Informatics, ICCCI 2020*.

<https://doi.org/10.1109/ICCCI48352.2020.9104094>

- Kumar, Kumar, A., & Palaparthi, V. S. (2021). Soil Sensors-Based Prediction System for Plant Diseases Using Exploratory Data Analysis and Machine Learning. *IEEE Sensors Journal*, 21(16), 17455–17468. <https://doi.org/10.1109/JSEN.2020.3046295>
- Kunertova, D. (2023). The war in Ukraine shows the game-changing effect of drones depends on the game. *Bulletin of the Atomic Scientists*, 79(2), 95–102. <https://doi.org/10.1080/00963402.2023.2178180>
- Labrie, J. W., & Earleywine, M. (2000). Sexual risk behaviors and alcohol: Higher base rates revealed using the unmatched-count technique. *The Journal of Sex Research* Nov, 37(4). <https://search-proquest-com.libproxy.ucl.ac.uk/docview/215279855/fulltextPDF/F42EEC066E514822PQ/1?accountid=14511>
- Labus, H. (2022). *Your CCTV devices can be hacked and weaponized*. Help Net Security. <https://www.helpnetsecurity.com/2022/10/27/cctv-hacks/>
- Lacinák, M., & Ristvej, J. (2017). Smart city, Safety and Security. *Procedia Engineering*, 192, 522–527. <https://doi.org/10.1016/j.proeng.2017.06.090>
- Ladegaard, I. (2019). Crime displacement in digital drug markets. *International Journal of Drug Policy*, 63, 113–121. <https://doi.org/10.1016/j.drugpo.2018.09.013>
- Langer, L., & Kammerstetter, M. (2015). Chapter 3 - The Evolution of the Smart Grid Threat Landscape and Cross-Domain Risk Assessment. In F. Skopik & P. B. T.-S. G. S. Smith (Eds.), *Smart Grid Security* (pp. 49–77). Syngress. <https://doi.org/https://doi.org/10.1016/B978-0-12-802122-4.00003-1>
- Laufs, J., & Borrión, H. (2021). Technological innovation in policing and crime prevention: Practitioner perspectives from London: <https://doi.org/10.1177/14613557211064053>, 146135572110640. <https://doi.org/10.1177/14613557211064053>
- Laufs, J., Borrión, H., & Bradford, B. (2020a). Security and the smart city: A systematic review. *Sustainable Cities and Society*, 55, 102023. <https://doi.org/10.1016/j.scs.2020.102023>
- Laufs, J., Borrión, H., & Bradford, B. (2020b). Security and the smart city: A systematic review. *Sustainable Cities and Society*, 55, Article 102023. (2020), 55. <https://doi.org/10.1016/J.SCS.2020.102023>
- Lee, I., Jung, S., Lee, J., & Macdonald, E. (2019). *Street crime prediction model based on the physical characteristics of a streetscape: Analysis of streets in low-rise housing areas in South Korea*. 46(5), 862–879. <https://doi.org/10.1177/2399808317735105>
- Lee, J. J., Go, M. H., Kim, Y. K., Joo, M., Seo, J., Oh, H., Kauh, J., & Lee, K. (2020). A multi-component analysis of cpted in the cyberspace domain. *Sensors (Basel, Switzerland)*, 20(14), 1–18. <https://doi.org/10.3390/s20143968>
- Lee, J., Kim, J., & Seo, J. (2019). Cyber attack scenarios on smart city and their ripple effects. *2019 International Conference on Platform Technology and Service (PlatCon)*, 1–5.

- Lee, J. Y., Kim, K. D., & Kim, K. (2019). A Study on Improving the Location of CCTV Cameras for Crime Prevention through an Analysis of Population Movement Patterns using Mobile Big Data [Article]. *KSCE Journal of Civil Engineering*, 23(1), 376–387. <https://doi.org/10.1007/s12205-018-1486-4>
- Lee, N., & Contreras, C. (2021). Neighborhood Walkability and Crime: Does the Relationship Vary by Crime Type? *Environment and Behavior*, 53(7), 753–786. <https://doi.org/10.1177/0013916520921843>
- Lee, Y., Eck, J. E., & Corsaro, N. (2016). Conclusions from the history of research into the effects of police force size on crime-1968 through 2013: a historical systematic review. *J Exp Criminol*, 12, 431–451. <https://doi.org/10.1007/s11292-016-9269-8>
- Legislation.gov.uk. (2021). *The Electric Vehicles (Smart Charge Points) Regulations 2021*. The National Archives. <https://www.legislation.gov.uk/ukxi/2021/1467/contents/made>
- Legislation.gov.uk. (2023). *Online Safety Act 2023*. The National Archives. <https://www.legislation.gov.uk/ukpga/2023/50>
- Legislation.gov.uk. (2024). *The Procurement Regulations 2024 No. 692*. <https://www.legislation.gov.uk/ukdsi/2024/9780348259728/contents>
- Lessambo, F. I. (2023). *The Cybersecurity Counteroffensive*. 11–32. https://doi.org/10.1007/978-3-031-23484-2_2
- Leukfeldt, E. R., Notté, R. J. (Raoul), & Malsch, M. (Marijke). (2020). Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. *Victims & Offenders*, 15(1), 60–77. <https://doi.org/10.1080/15564886.2019.1672229>
- Levi, M., Doig, A., Gundur, R., Wall, D., Williams, M., & Levi, M. (2017). Cyberfraud and the implications for effective risk-based responses: themes from UK research. *Crime, Law and Social Change*, 67, 77–96. <https://doi.org/10.1007/s10611-016-9648-0>
- Levy, M. P., & Tartaro, C. (2010). Auto Theft: A Site-Survey and Analysis of Environmental Crime Factors in Atlantic City, NJ. *Security Journal*, 23, 75–94. <https://doi.org/10.1057/palgrave.sj.8350088>
- Lewis Sharon. (2021, May 16). *Reimagining Cities: Why streetscape is essential to urban design*. Cityscape. <https://www.cityscape-intelligence.com/architecture/reimagining-cities-why-streetscape-essential-urban-design>
- LGA. (2019). *A councillor's guide to procurement 2019 edition*. https://research.local.gov.uk/jfe/form/SV_
- Li, J., Li, N., Peng, J., Cui, H., & Wu, Z. (2019). Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies. *Energy*, 168, 160–168. <https://doi.org/https://doi.org/10.1016/j.energy.2018.11.046>
- Li, W., Song, H., & Zeng, F. (2018). Policy-Based Secure and Trustworthy Sensing for Internet of Things in Smart Cities. *IEEE Internet of Things Journal*, 5(2), 716–723. <https://doi.org/10.1109/JIOT.2017.2720635>
- Liggett Anastasia Loukaltou-Slderis, R. H., & Isekl, R. (2003). *Bus Stop-Environmental*

Connection: Do Characteristics of the Built Environment Correlate with Bus Stop Crime? <https://escholarship.org/uc/item/7w66d9nz>

- Lim, H.-W. (2021). A Study on Countermeasures Against Cyber Infringement Considering CPTED. *International Journal of Advanced Culture Technology*, 9(2), 106–117.
- Lim, H., Kim, C., Eck, J. E., & Kim, J. (2016). The crime-reduction effects of open-street CCTV in South Korea. *Security Journal*, 29(2), 241–255. <https://doi.org/10.1057/sj.2013.10>
- Lim, H., & Wilcox, P. (2017). Crime-Reduction Effects of Open-street CCTV: Conditionality Considerations. *Justice Quarterly*, 34(4), 597–626. <https://doi.org/10.1080/07418825.2016.1194449>
- Lipsey, M., & Wilson, D. (1961). *Practical meta-analysis* / Mark W. Lipsey, David B. Wilson. Thousand Oaks, Calif.; London: SAGE. https://ucl-new-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=UCL_LMS_DS21129370740004761&context=L&vid=UCL_VU2&lang=en_US&search_scope=CSCOP_UCL&adaptor=Local Search Engine&isFrbr=true&tab=local&query=any,contains,wilson and lipsey&sortb
- Liu, L., & Eck, J. (2008). *Artificial crime analysis systems : using computer simulations and geographic information systems*. Information Science Reference.
- Liu, L., Lan, M., Eck, J. E., Yang, B., & Zhou, H. (2020). Assessing the Intraday Variation of the Spillover Effect of Tweets-Derived Ambient Population on Crime. *Social Science Computer Review*, 40(2), 512–533. <https://doi.org/10.1177/0894439320983825>
- Local Government Association. (2017). *National technological and digital procurement category strategy*.
- Local Government Association. (2019). *A councillor's guide to procurement*. https://www.local.gov.uk/sites/default/files/documents/11.169_A_Councillors_Guide_to_Procurement_03 WEB.pdf
- Lockwood, D. (2007). Mapping Crime in Savannah Social Disadvantage, Land Use, and Violent Crimes Reported to the Police. *Social Science Computer Review*, 25. <https://doi.org/10.1177/0894439307298935>
- Loia, F., & Maione, G. (2022). Social Accountability of Local Governments in Smart Cities: A Multiple Case Study. In *Managing Smart Cities: Sustainability and Resilience Through Effective Management* (pp. 181–197). Springer.
- Lopes, N. V. (2017). Smart governance: A key factor for smart cities implementation. *2017 IEEE International Conference on Smart Grid and Smart Cities (ICSGSC)*, 277–282.
- Lopez-Fuentes, L., van de Weijer, J., González-Hidalgo, M., Skinnemoen, H., & Bagdanov, A. D. (2018). Review on computer vision techniques in emergency situations [Article]. *Multimedia Tools and Applications*, 77(13), 17069–17107. <https://doi.org/10.1007/s11042-017-5276-7>
- LOTI. (2020a). *Electric Vehicle (EV) Charge Points Dashboard*. <https://loti.london/projects/ev-charge-points/>

- LOTI. (2020b). *London Office of Technology and Innovation*. <https://loti.london/>
- LOTI. (2021). *Innovation in Procurement*. <https://loti.london/projects/innovation-in-procurement/>
- Loukaitou-Sideris, A. (2012). Safe on the move: The importance of the built environment. In *The Urban Fabric of Crime and Fear* (pp. 85–110). Springer Netherlands. https://doi.org/10.1007/978-94-007-4210-9_4
- Luppigini, R., & So, A. (2016). A technoethical review of commercial drone use in the context of governance, ethics, and privacy. *Technology in Society*, 46, 109–119. <https://doi.org/10.1016/J.TECHSOC.2016.03.003>
- Ma, T., Motta, G., & Liu, K. (2017). Delivering Real-Time Information Services on Public Transit: A Framework. *IEEE Transactions on Intelligent Transportation Systems*, 18(10), 2642–2656. <https://doi.org/10.1109/TITS.2017.2656387>
- Macaulay, T. (2016). Chapter 12 - Threats and Impacts to the IoT. In *RIoT Control* (pp. 221–278). Elsevier Science & Technology.
- Macdonald, J. M., Nicosia, N., Benjamin, •, Ukert, D., & Org, N. (2018). Do Schools Cause Crime in Neighborhoods? Evidence from the Opening of Schools in Philadelphia. *J Quant Criminol*, 34, 717–740. <https://doi.org/10.1007/s10940-017-9352-y>
- MacDonald, J. M., Nicosia, N., & Ukert, B. D. (2018). Do Schools Cause Crime in Neighborhoods? Evidence from the Opening of Schools in Philadelphia. *Journal of Quantitative Criminology*, 34(3), 717–740. <https://doi.org/10.1007/s10940-017-9352-y>
- Maglaras, L., Drivas, G., Noou, K., & Rallis, S. (2018). *NIS directive: The case of Greece*. <https://doi.org/10.4108/eai.15-5-2018.154769>
- Maimon, D., & Louderback, E. R. (2019). Cyber-Dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology*, 2(1), 191–216. <https://doi.org/10.1146/annurev-criminol-032317-092057>
- Malik, A. W., & Anwar, Z. (2022). Do Charging Stations Benefit from Cryptojacking? A Novel Framework for Its Financial Impact Analysis on Electric Vehicles. *Energies*, 15(16), 5773. <https://www.mdpi.com/1996-1073/15/16/5773>
- Management, A. R. of D., Service, N. U. of P., Budapest, & Hungary. (2015). Drone Applications for Supporting Disaster Management. *World Journal of Engineering and Technology*, 03(03), 316–321. <https://doi.org/10.4236/WJET.2015.33C047>
- Marcucci, E., Le Pira, M., Carrocci, C. S., Gatta, V., & Pieralice, E. (2017). Connected shared mobility for passengers and freight: Investigating the potential of crowdshipping in urban areas. *5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems, MT-ITS 2017 - Proceedings*, 839–843. <https://doi.org/10.1109/MTITS.2017.8005629>
- Markets and Markets. (2022). *Video Surveillance Market*. <https://www.marketsandmarkets.com/PressReleases/uk-global-video-surveillance-market.asp>
- Marquet, O., Hipp, J. A., Alberico, C., Huang, J.-H., Fry, D., Mazak, E., Lovasi, G. S.,

- & Floyd, M. F. (2019). Short-term associations between objective crime, park-use, and park-based physical activity in low-income neighborhoods. *Preventive Medicine*, 126, 105735. <https://doi.org/https://doi.org/10.1016/j.ypmed.2019.05.023>
- Martin, R. (2013). Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge. *International Journal of Intelligence and CounterIntelligence*, 26(3), 453–481. <https://doi.org/10.1080/08850607.2013.780552>
- Maulana, L. R., Fajar, A. N., & Meyliana. (2019). Designing a Smart Mobile Application to Detect Fraud Theft of E-Banking Access Based on SOA In Indonesia. *ICTSS*, 7, 1–4. <https://doi.org/10.1109/ICISS48059.2019.8969848>
- Mcglinn, J., Bell, E. F., Downing, J. F., & Cook, E. M. (2011). An exploration of 1st and 2nd generation CPTED for end of year school leavers at Rottneest Island. *4th Australian Security and Intelligence Conference*, 5–7. <https://doi.org/10.4225/75/57a0110cac5c2>
- McGrath, M. J. (2004). Promoting walking and cycling as an alternative to using cars: comfort of cycling needs to be akin to that of using cars. In *BMJ (Clinical research ed.)* (Vol. 329, Issue 7476). <https://doi.org/10.1136/bmj.329.7476.1237-a>
- McKinlay, P. (2017). Make way for smart cities: opportunities, challenges and capacities of New Zealand local governments [Article]. *Asia Pacific Journal of Public Administration = Ya Tai Gong Gong Xing Zheng Xue*, 39(4), 297–303. <https://doi.org/10.1080/23276665.2017.1405627>
- Meijer, A. (2018). Datapolis: A Public Governance Perspective on “Smart Cities.” *Perspectives on Public Management and Governance*, 1(3), 195–206. <https://doi.org/10.1093/ppmgov/gvx017>
- Metere, R., Pourmirza, Z., Walker, S., & Neaimah, M. (2022). An Overview of Cyber Security and Privacy on the Electric Vehicle Charging Infrastructure. *ArXiv Preprint ArXiv:2209.07842*.
- Michael, B., V., H. L., & Julian P. T. Higgins, H. R. R. (2011). *Introduction to Meta-Analysis*. Wiley Publishers. https://books.google.co.uk/books?hl=en&lr=&id=JQg9jdrq26wC&oi=fnd&pg=PT14&dq=meta-analysis++&ots=VJZVTRIDit&sig=fTGXnLFkdP4RQ6ixtPx2oLjx2k&redir_esc=y#v=onepage&q=meta-analysis&f=false
- Mihale-Wilson, C. A., Felka, P., & Hinz, O. (2019). “The Bright and the Dark Side of Smart Lights” The Protective Effect of Smart City Infrastructures. *Hawaii International Conference on System Sciences*. <https://api.semanticscholar.org/CorpusID:102350844>
- Mihinjac, M., & Saville, G. (2019). Third-generation crime prevention through environmental design (CPTED). *Social Sciences*, 8(6). <https://doi.org/10.3390/socsci8060182>
- Mijac, M., Androcec, D., & Picek, R. (2017). SMART CITY SERVICES DRIVEN BY IOT: A SYSTEMATIC REVIEW. In *SMART CITY SERVICES DRIVEN BY IOT: A SYSTEMATIC REVIEW Journal of Economic and Social Development* (Vol. 4, Issue 2). <https://search-proquest->

com.libproxy.ucl.ac.uk/docview/1951427121/fulltextPDF/E926680201A740CEP
Q/1?accountid=14511

- Milenkovic, M., Rasic, M., & Jovancevic, R. (2022). Public Procurement of Innovative and Technological Solutions in the EU [Proceeding]. *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, 1258–1263.
<https://doi.org/10.23919/MIPRO55190.2022.9803368>
- Miller, J. (2012). Individual Offending, Routine Activities, and Activity Settings: Revisiting the Routine Activity Theory of General Deviance. *Journal of Research in Crime and Delinquency*, 50(3), 390–416.
<https://doi.org/10.1177/0022427811432641>
- Millonig, A., & Gartner, G. (2010). Identifying motion and interest patterns of shoppers for developing personalised wayfinding tools. *Https://Doi.Org/10.1080/17489725.2010.535029*, 5(1), 3–21.
<https://doi.org/10.1080/17489725.2010.535029>
- Mirea, M., Wang, V., & Jung, J. (2019). The not so dark side of the darknet: a qualitative study. *Security Journal*, 32(2), 102–118.
<https://doi.org/10.1057/s41284-018-0150-5>
- Miró Llinares, F., & Johnson, S. D. (2018a). *Cybercrime and Place: Applying Environmental Criminology to Crimes in Cyberspace* (pp. 883–906). Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780190279707.013.39>
- Miró Llinares, F., & Johnson, S. D. (2018b). Cybercrime and Place. In *The Oxford Handbook of Environmental Criminology* (Vol. 1, Issue February, pp. 1–27). <https://doi.org/10.1093/oxfordhb/9780190279707.013.39>
- Mitchell, C. (2012). *The cyber crime threat on mobile devices*. <http://sourceforge.net/projects/airjack/>
- Moellers, N., & Haelterlein, J. (2013). Privacy issues in public discourse: the case of “smart” CCTV in Germany [Article]. *Innovation (Abingdon, England)*, 26(1–2), 57–70. <https://doi.org/10.1080/13511610.2013.723396>
- Monahan, T. (2009). Identity theft vulnerability. *Theoretical Criminology*, 13(2), 155–176. <https://doi.org/10.1177/1362480609102877>
- Monchuk, L., & Clancey, G. (2013). Designing out Crime - Voices from the Fields: Editorial for Special Edition of Safer Communities. *Safer Communities*, 12(4). <http://eprints.hud.ac.uk/id/eprint/17990/>
- Mookerjee, S. (2022, May 9). *EV infrastructure vulnerabilities put cars, the grid at risk* - GCN. Government Computer News (GCN). <https://gcn.com/cybersecurity/2022/05/ev-infrastructure-vulnerabilities-put-cars-grid-risk/366694/>
- Moon, T.-H., Heo, S.-Y., & Lee, S.-H. (2014). Ubiquitous Crime Prevention System (UCPS) for a Safer City. *Procedia Environmental Sciences*, 22, 288–301. <https://doi.org/10.1016/j.proenv.2014.11.028>
- MORE. (2018). *Future scenarios for TEN feeder routes*.

- MORE. (2022a). *Better Streets for Better Cities: Summary and Key Recommendations*. <https://www.roadspace.eu/results/better-streets-for-better-cities-summary-and-key-recommendations>
- MORE. (2022b). *Deliverable D3.1 Analysis of Technological Advances*. <https://morelive.wpenginpowered.com/wp-content/uploads/2022/04/MORE-WP3-D3.1-technological-advances-v07.pdf>
- MORE. (2022c). *MORE Deliverables*. <https://www.roadspace.eu/results/more-deliverables>
- MORE project. (2023). *MORE Deliverables*. European Union's Horizon 2020 Research and Innovation Programme. <https://www.roadspace.eu/results/more-deliverables>
- Mouli, G. R. C., Venugopal, P., & Bauer, P. (2017). Future of electric vehicle charging. *2017 International Symposium on Power Electronics (Ee)*, 1–7. <https://doi.org/10.1109/PEE.2017.8171657>
- Mughal, R., DeMarinis, V., Nordendahl, M., Lone, H., Phillips, V., & Boyd-MacMillan, E. (2023). Public Mental Health Approaches to Online Radicalisation: An Empty Systematic Review. *International Journal of Environmental Research and Public Health*, 20(16), 6586. <https://doi.org/10.3390/ijerph20166586>
- Muncaster, P. (2019, August 23). *City of London Hit by One Million Cyber-Attacks Per Month*. Infosecurity Magazine. <https://www.infosecurity-magazine.com/news/city-of-london-one-million/>
- Muncaster, P. (2023). *NIS 2 is Coming: Here's What UK Organisations Need to Know*. Isms.Online. <https://www.isms.online/information-security/nis-2-is-coming-heres-what-uk-organisations-need-to-know/#:~:text=But time is the enemy,will diverge from NIS 2.>
- Munn, Z., Peters, M. D. J., Stern, C., Tufanaru, C., McArthur, A., & Aromataris, E. (2018). Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. *BMC Medical Research Methodology*, 18(1), 143. <https://doi.org/10.1186/s12874-018-0611-x>
- Murad, D. F., Abbas, B. S., Trisetyarso, A., Suparta, W., & Kang, C. H. (2018). Development of smart public transportation system in Jakarta city based on integrated IoT platform. *2018 International Conference on Information and Communications Technology, ICOIACT 2018, 2018-January*, 872–877. <https://doi.org/10.1109/ICOIACT.2018.8350812>
- Myers West, S. (2018). Censored, suspended, shadowbanned: User interpretations of content moderation on social media platforms. *New Media & Society*, 20(11), 4366–4383.
- Nabi, S. T., Kumar, M., Singh, P., Aggarwal, N., & Kumar, K. (2022). A comprehensive survey of image and video forgery techniques: variants, challenges, and future directions [Article]. *Multimedia Systems*, 28(3), 939–992. <https://doi.org/10.1007/s00530-021-00873-8>
- Nápoles, V. M. P., Páez, D. G., Penelas, J. L. E., Pérez, O. G., Santacruz, M. J. G., & de Pablos, F. M. (2020). Smart bus stops as interconnected public spaces for

- increasing social inclusiveness and quality of life of elder users [Article]. *Smart Cities (Basel)*, 3(2), 430–443. <https://doi.org/10.3390/smartcities3020023>
- Nasr, T., Torabi, S., Bou-Harb, E., Fachkha, C., & Assi, C. (2022). Power jacking your station: In-depth security analysis of electric vehicle charging station management systems. *Computers & Security*, 112, 102511. <https://doi.org/https://doi.org/10.1016/j.cose.2021.102511>
- Nasr, T., Torabi, S., Bou-Harb, E., Fachkha, C., & Assi, C. (2023). ChargePrint: A Framework for Internet-Scale Discovery and Security Analysis of EV Charging Management Systems. *NDSS*.
- National Cyber Security Centre - Government of Ireland. (2022). *National Cyber Risk Assessment*. <https://assets.gov.ie/261044/1389e6d2-6d48-40e0-a97a-bf9396c70386.pdf>
- National Cybersecurity center of Excellence. (2000). *Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure*. NIST. <https://www.nccoe.nist.gov/projects/cybersecurity-framework-profile-electric-vehicle-extreme-fast-charging-infrastructure>
- National Protective Security Authority (NPSA). (2023). *Connected Places: related legislation, regulations & guidance*. <https://www.npsa.gov.uk/system/files/documents/connected-places-related-legislation-regulations-guidance.pdf>
- NCSC. (2021a, May). *Connected Places Cyber Security Principles*. <https://www.ncsc.gov.uk/files/NCSC-Connected-Places-security-principles-May-2021.pdf>
- NCSC. (2021b, May 7). *Connected Places Cyber Security Principles - NCSC.GOV.UK*. <https://www.ncsc.gov.uk/collection/connected-places-security-principles>
- NCSC. (2022a). *NCSC Annual Review*. <https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf>
- NCSC. (2022b, April 11). *NCSC CAF guidance - NCSC.GOV.UK*. <https://www.ncsc.gov.uk/collection/caf>
- NCSC. (2022c, December 15). *National Cyber Strategy 2022 - GOV.UK*. <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022>
- Nedelea, A. (2022). *Study: Hybrids, ICE Cars Far More Likely Than EVs To Catch Fire*. InsideEVs. <https://insideevs.com/news/561549/study-evs-smallest-fire-risk/>
- NESCOR. (2015). *Electric Sector Failure Scenarios and Impact Analyses-Version 3.0 National Electric Sector Cybersecurity Organization Resource (NESCOR)*. <https://smartgrid.epri.com/doc/NESCOR Failure Scenarios v3 12-11-15.pdf>
- Newman, O. (1972). *Defensible space : crime prevention through urban design / Oscar Newman*. New York : Macmillan.
- Newton, A. (2008). A study of bus route crime risk in urban areas: The changing environs of a bus journey. *Built Environment*, 34(1), 88–103.

<https://doi.org/10.2148/benv.34.1.88>

- Newton, A. D., Partridge, H., & Gill, A. (2014a). In and around: Identifying predictors of theft within and near to major mass underground transit systems. *Security Journal*, 27, 132–146. <https://doi.org/10.1057/sj.2014.2>
- Newton, A. D., Partridge, H., & Gill, A. (2014b). Above and below: measuring crime risk in and around underground mass transit systems. *Crime Science*, 3(1), 1. <https://doi.org/10.1186/2193-7680-3-1>
- Newton, A. D., Partridge, H., & Gill, A. (2014c). Above and below: measuring crime risk in and around underground mass transit systems. *Crime Science*, 3(1), 1. <https://doi.org/10.1186/2193-7680-3-1>
- Neyeloff, J. L., Fuchs, S. C., & Moreira, L. B. (2012). Meta-analyses and Forest plots using a microsoft excel spreadsheet: Step-by-step guide focusing on descriptive data analysis. *BMC Research Notes*, 5(1), 52. <https://doi.org/10.1186/1756-0500-5-52>
- Nicol, D. M. (2005). Modeling and simulation in security evaluation. *IEEE Security & Privacy*, 3(5), 71–74.
- Niranjan Ajit. (2022, July 3). *War highlights energy systems vulnerability – DW – 03/07/2022. Nature and ~Environment | Germany.* <https://www.dw.com/en/cybersecurity-electricity-russia-hackers/a-61037938>
- Nisar, F., Ramachandran, G., Vilathgamuva, M., & Jurdak, R. (2022). Manipulation of Actual Demand in Electric Vehicles (MaD EV): A Cyber-Security Perspective. *2022 IEEE 7th Southern Power Electronics Conference (SPEC)*, 1–8. <https://doi.org/10.1109/SPEC55080.2022.10058269>
- NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. <https://doi.org/10.6028/NIST.CSWP.04162018>
- NIST. (2023). *NIST Computer Security Resource Center*. Initiative, Joint Task Force Transformation. <https://csrc.nist.gov/publications/sp800>
- O'Halloran, J. (2020). *More than 30 million smart street lights by 2023, predicts study.* Computer Weekly. <https://www.computerweekly.com/news/252476290/More-than-30-million-smart-street-lights-by-2023-predicts-study>
- O'Malley, P., & Smith, G. J. (2022). 'Smart' crime prevention? Digitization and racialized crime control in a Smart City [Article]. *Theoretical Criminology*, 26(1), 40–56. <https://doi.org/10.1177/1362480620972703>
- O'SULLIVAN-DALE, U. (2022, October 24). *UK public EV charging network to double in size by 2023, research finds | CiTTi Magazine.* City Transport and Traffic Innovation (CiTTi). <https://www.cittimagazine.co.uk/uncategorized/uk-public-ev-charging-network-to-double-in-size-by-2023-research-finds.html>
- O'Sullivan, F. (2021). *Make Way for the 'One-Minute City.'* Bloomberg. <https://www.bloomberg.com/news/features/2021-01-05/a-tiny-twist-on-street-design-the-one-minute-city>
- Offenhuber, D., & Schechtner, K. (2018). Improstructure - an improvisational perspective on smart infrastructure governance [Article]. *Cities*, 72, 329–338.

<https://doi.org/10.1016/j.cities.2017.09.017>

- Office for National Statistics-a. (2011). *Census geography*. [https://www.ons.gov.uk/methodology/geography/ukgeographies/censusgeography#:~:text=Merges were applied where%3A,5%2C000 people or 2%2C000 households](https://www.ons.gov.uk/methodology/geography/ukgeographies/censusgeography#:~:text=Merges%20were%20applied%20where%3A,5%2C000%20people%20or%202%2C000%20households)
- OfGem. (2023). Electric Vehicle Smart Charging Action Plan Affordable, sustainable power for electric vehicles. *Department of Business, Energy & Industrial Strategy (BEIS)*.
- Ogilvie, D., Egan, M., Hamilton, V., & Petticrew, M. (2004). Promoting walking and cycling as an alternative to using cars: Systematic review. In *British Medical Journal* (Vol. 329, Issue 7469, pp. 763–766). BMJ Publishing Group. <https://doi.org/10.1136/bmj.38216.714560.55>
- Omar, A., AlMaeen, S., Attia, H., Takruri, M., Altunajji, A., Sanduleanu, M., Shubair, R., Ashhab, M. S., Al Ali, M., & Al Hebsi, G. (2022). Smart City: Recent Advances in Intelligent Street Lighting Systems Based on IoT [Article]. *Journal of Sensors*, 2022, 1–10. <https://doi.org/10.1155/2022/5249187>
- Omer, I., & Kaplan, N. (2019). Structural properties of the angular and metric street network's centralities and their implications for movement flows. *Environment and Planning. B, Urban Analytics and City Science*, 46(6), 1182–1200. <https://doi.org/10.1177/2399808318760571>
- Öörni, R., & Goulart, A. (2017). In-Vehicle Emergency Call Services: ECall and beyond. *IEEE Communications Magazine*, 55(1), 159–165. <https://doi.org/10.1109/MCOM.2017.1600289CM>
- Orabi, A. (2024). The Effect Of Dark Web On National And International Security. *Library Progress International*, 44(3), 18057–18070.
- Owano Nancy. (2017, October 10). *Prototype offers dynamic approach to pedestrian crossing*. Tech Xplore. <https://techxplore.com/news/2017-10-prototype-dynamic-approach-pedestrian.html>
- Oztemel, E., & Gursev, S. (2020). Literature review of Industry 4.0 and related technologies. *Journal of Intelligent Manufacturing*, 31(1), 127–182. <https://doi.org/10.1007/s10845-018-1433-8>
- Painter, K., & Farrington, D. P. (1999). Improved Street Lighting: Crime Reducing Effects and Cost-Benefit Analyses. *Security Journal*, 12(4), 17. <https://doi.org/https://doi.org/10.1057/palgrave.sj.8340037>
- Palleti, V. R., Adep, S., Mishra, V. K., & Mathur, A. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. *Cybersecurity*, 4(1), 8. <https://doi.org/10.1186/s42400-021-00071-z>
- Papaiakovou, A., Nika, C., & Vergados, D. D. (2022). E-Privacy Issues in the Smart Cities Environment. *13th International Conference on Information, Intelligence, Systems and Applications, IISA 2022*. <https://doi.org/10.1109/IISA56318.2022.9904395>
- Pardo-Bosch, F., Blanco, A., Sesé, E., Ezcurra, F., & Pujadas, P. (2022). Sustainable strategy for the implementation of energy efficient smart public lighting in urban

- areas: case study in San Sebastian. *Sustainable Cities and Society*, 76, 103454. <https://doi.org/https://doi.org/10.1016/j.scs.2021.103454>
- Pareek, S., Sujil, A., Ratna, S., & Kumar, R. (2020). Electric Vehicle Charging Station Challenges and Opportunities: A Future Perspective. *2020 International Conference on Emerging Trends in Communication, Control and Computing (ICONC3)*, 1–6. <https://doi.org/10.1109/ICONC345789.2020.9117473>
- Park, J. (2022). *Measuring Public Life Through Digital Technologies: Investigating the Use of WiFi Sensing for Enhancing Public Space*. <https://scholarworks.unist.ac.kr/handle/201301/57551>
- Pasha, H. (2020, September 21). *Smart Cities could save the world – until there's a cybersecurity emergency - Smart Cities World*. SmartCitiesWorld. <https://www.smartcitiesworld.net/opinions/smart-cities-could-save-the-world--until-theres-a-cybersecurity-emergency>
- Pawłowski, P., Dąbrowski, A., Balcerek, J., Konieczka, A., & Piniarski, K. (2020). Visualization techniques to support CCTV operators of smart city services. *Multimedia Tools and Applications*, 79(29–30), 21095–21127. <https://doi.org/10.1007/S11042-020-08895-6>
- pbctoday. (2017). *Secured by Design: Tackling crime through the built environment*. Pbctoday. <https://www.pbctoday.co.uk/news/building-control-news/secured-by-design-tackling-crime-through-the-built-environment/36696/>
- Pearlstein, A., & Wachs, M. (1982). Crime in public transit systems: An environmental design perspective. *Transportation*, 11(3), 277–297. <https://doi.org/10.1007/BF00172653>
- Pease, K. (1998). *Repeat Victimisation: Taking Stock*. https://popcenter.asu.edu/sites/default/files/problems/domestic_violence/PDFs/Pease_1998.pdf
- Peršak, N. (2021). Offending sights and urban governance: Expectations of city aesthetics and spatial responses to the unsightly. In *Harm and disorder in the Urban space* (pp. 52–77). Routledge.
- Petkauskas, V. (2021). *Report: number of expert-crafted video deepfakes double every six months*. CyberNews. <https://cybernews.com/privacy/report-number-of-expert-crafted-video-deepfakes-double-every-six-months/>
- Petrini, K., McAleer, P., Neary, C., Gillard, J., & Pollick, F. E. (2014). Experience in judging intent to harm modulates parahippocampal activity: An fMRI study with experienced CCTV operators. *Cortex*, 57, 74–91. <https://doi.org/10.1016/J.CORTEX.2014.02.026>
- Phillips, T. (2017). *THE CAPABILITIES AND JURISDICTIONS OF FEDERAL AGENCIES OF THE UNITED STATES GOVERNMENT IN CYBER-CRIME RESPONSE*.
- Phiri, L., Tembo, S., & Nyoni, K. J. (2022). Assessing the Ramifications of Electric Vehicle Charging Infrastructure on Smart Grid Systems in Zambia. *2022 International Conference on Information and Communication Technology for Development for Africa (ICT4DA)*, 175–180.

- Pirootfar, P., Farr, E. R. P., Aboagye-Nimo, E., & Osei-Berchie, J. (2019). Crime prevention in urban spaces through environmental design: A critical UK perspective. *Cities*, 95, 102411. <https://doi.org/10.1016/j.cities.2019.102411>
- Pitcher, A. B., & Johnson, S. D. (2011). Exploring Theories of Victimization Using a Mathematical Model of Burglary. *Journal of Research in Crime and Delinquency*, 48(1), 83–109. <https://doi.org/10.1177/0022427810384139>
- Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019a). CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology and Public Policy*, 18(1), 135–159. <https://doi.org/10.1111/1745-9133.12419>
- Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019b). CCTV surveillance for crime prevention. *Criminology & Public Policy*, 18(1), 135–159. <https://doi.org/10.1111/1745-9133.12419>
- Pizzuti, S., Annunziato, M., & Moretti, F. (2013). Smart street lighting management. *Energy Efficiency*, 6(3), 607–616. <https://doi.org/10.1007/S12053-013-9195-9>
- Plaka, R., Asplund, M., & Nadjm-Tehrani, S. (2023). *Vulnerability analysis of an electric vehicle charging ecosystem*.
- Plexal. (n.d.). *Secure Connected Places research project - Plexal*. Retrieved January 25, 2023, from <https://www.plexal.com/secure-connected-places/>
- Plexal on behalf of DSIT. (2023). *Secure Connected Places, International Evidence Project*. https://assets.publishing.service.gov.uk/media/64954668831311001329622f/secure_connected_places_international_evidence_project.pdf
- Pourmirza, Z., & Walker, S. (2021). Electric Vehicle Charging Station: Cyber Security Challenges and Perspective. *2021 9th IEEE International Conference on Smart Energy Grid Engineering, SEGE 2021*, 111–116. <https://doi.org/10.1109/SEGE52446.2021.9535052>
- Prasad. (2009). (12) *United States Patent* (45) *Date of Patent*: (54) *SIGNAL CONDITIONER AND METHOD FOR COMMUNICATING OVER A SHARED TRANSPORT MEDIUM COMBINED DIGITAL SIGNAL FOR WIRELESS SERVICE*. <http://en.wikipedia.org/wiki/>
- Pratt, R. M., & Carroll, T. E. (2019). Vehicle Charging Infrastructure Security. *2019 IEEE International Conference on Consumer Electronics (ICCE)*, 1–5. <https://doi.org/10.1109/ICCE.2019.8662043>
- Pribyl, P., & Pribyl, O. (2015). Definition of a smart street as smart city's building element. *2015 Smart Cities Symposium Prague (SCSP)*, 1–6. <https://doi.org/10.1109/SCSP.2015.7181575>
- Prichard, J., Wortley, R., Watters, P., Spiranovic, C., & Scanlan, J. (2024). The effect of therapeutic and deterrent messages on Internet users attempting to access 'barely legal' pornography. *Child Abuse & Neglect*, 155, 106955. <https://doi.org/10.1016/j.chiabu.2024.106955>
- Pridemore, W. A., & Grubestic, T. H. (2013). Alcohol Outlets and Community Levels of Interpersonal Violence: Spatial Density, Outlet Type, and Seriousness of Assault.

- Journal of Research in Crime and Delinquency*, 50(1), 132–159. <https://doi.org/10.1177/0022427810397952>
- Priporas, C. V., Stylos, N., & Fotiadis, A. K. (2017). Generation Z consumers' expectations of interactions in smart retailing: A future agenda. *Computers in Human Behavior*, 77, 374–381. <https://doi.org/10.1016/J.CHB.2017.01.058>
- Prislan, K., & Slak, B. (2018). *Analysis of the Relationship Between Smart Cities, Policing and Criminal Investigation*. <https://search-proquest-com.libproxy.ucl.ac.uk/docview/2168048715/fulltextPDF/6C0A6F36C4104347PQ/1?accountid=14511>
- Proquest LLC. (2020). *Proquest*. <https://about.proquest.com/en/content-solutions/databases/>
- Qin, X., & Liu, L. (2016). Evaluating the Relationships of Bus Transit with Street and Off-Street Robberies. *Professional Geographer*, 68(2), 227–237. <https://doi.org/10.1080/00330124.2015.1059400>
- Quick, M., Law, J., & Luan, H. (2017). The Influence of On-Premise and Off-Premise Alcohol Outlets on Reported Violent Crime in the Region of Waterloo, Ontario: Applying Bayesian Spatial Modeling to Inform Land Use Planning and Policy. *Applied Spatial Analysis and Policy*, 10(3), 435–454. <https://doi.org/10.1007/s12061-016-9191-5>
- Rahman, M. F. B. A. (2022). *Chapter 3. Issues and Challenges*. S. Rajaratnam School of International Studies. <https://www-jstor-org.libproxy.ucl.ac.uk/stable/resrep05940?sid=primo>
- Rajesh, K. V. N., & Ramesh, K. V. N. (2016). Computer Forensics: An Overview. *I-Manager's Journal on Software Engineering*, 10(4), 1–5. <https://search.proquest.com/docview/1816335831?accountid=14511>
- Rajkumar, V. S., Stefanov, A., Torres, J. L. R., & Palensky, P. (2024). Dynamical Analysis of Power System Cascading Failures Caused by Cyber Attacks. *IEEE Transactions on Industrial Informatics*.
- Raman, G., AlShebli, B., Waniek, M., Rahwan, T., & Peng, J. C. H. (2020). How weaponizing disinformation can bring down a city's power grid. *PLOS ONE*, 15(8), e0236517. <https://doi.org/10.1371/JOURNAL.PONE.0236517>
- Ratcliffe, J. H. (2012). *The Spatial Extent of Criminogenic Places: A Change-point Regression of Violence around Bars*. <https://doi.org/10.1111/j.1538-4632.2012.00856.x>
- Redwood, F. (2023). *Oxford, Bristol and Sheffield are all embracing the 15-minute city: But is the walkable “urban village” concept a boon or a curse?* Daily Mail. <https://www.dailymail.co.uk/property/article-11921133/Oxford-Bristol-Sheffield-embrace-15-minute-city-concept-boon-curse.html>
- Reeh, D., Cruz Tapia, F., Chung, Y.-W., Khaki, B., Chu, C., & Gadh, R. (2019). Vulnerability Analysis and Risk Assessment of EV Charging System under Cyber-Physical Threats. *2019 IEEE Transportation Electrification Conference and Expo (ITEC)*, 1–6. <https://doi.org/10.1109/ITEC.2019.8790593>
- Rege, A. (2014). A Criminological Perspective on Power Grid Cyber attacks: Using

- Routine Activities Theory to Rational Choice Perspective to Explore Adversarial Decision-Making. *Journal of Homeland Security and Emergency Management*, 11(4), 463–487. <https://doi.org/10.1515/jhsem-2013-0061>
- Rehak, D., Senovsky, P., Hromada, M., Lovecek, T., & Novotny, P. (2018). Cascading impact assessment in a critical infrastructure system. *International Journal of Critical Infrastructure Protection*, 22, 125–138.
- Rejeb, A., Rejeb, K., Simske, S., Treiblmaier, H., & Zailani, S. (2022). The big picture on the internet of things and the smart city: a review of what we know and what we need to know. *Internet of Things*, 19, 100565.
- Remrey, L. P., & Maimon, D. (2016). *SURVEILLANCE IN CYBERSPACE: APPLYING NATURAL AND PLACE MANAGER SURVEILLANCE TO SYSTEM TRESPASSING*.
- Renalds, A., Smith, T. H., & Hale, P. J. (2010). A Systematic Review of Built Environment and Health. *Family & Community Health*, 33(1), 68–78. <https://doi.org/10.1097/FCH.0b013e3181c4e2e5>
- Renda, W., & Zhang, C. H. (2019). Comparative analysis of firearm discharge recorded by gunshot detection technology and calls for service in Louisville, Kentucky. *ISPRS International Journal of Geo-Information*, 8(6), 275. <https://doi.org/10.3390/ijgi8060275>
- Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention and Community Safety*, 12(2), 99–118. <https://doi.org/10.1057/cpcs.2009.22>
- Riadi, I., Siregar, A. A., Pratiwi, A. G., & others. (2022). Security on Charity Crowdfunding Services using KAMI Index 4.1. *Engineering Science Letter*, 1(01), 15–19.
- Ridgeway, G., & Macdonald, J. M. (2017a). Effect of Rail Transit on Crime: A Study of Los Angeles from 1988 to 2014. *Journal of Quantitative Criminology*, 33, 277–291. <https://doi.org/10.1007/s10940-016-9296-7>
- Ridgeway, G., & Macdonald, J. M. (2017b). Effect of Rail Transit on Crime: A Study of Los Angeles from 1988 to 2014. *J Quant Criminol*, 33, 277–291. <https://doi.org/10.1007/s10940-016-9296-7>
- Riley, T. (2021). The Cybersecurity 202: Cybercrime skyrocketed as workplaces went virtual in 2020, new report finds [Article]. *The Washington Post* (Washington, D.C. 1974. Online).
- Roberto, E. (2018). Analysis of Residential Segregation THE SPATIAL PROXIMITY AND CONNECTIVITY METHOD FOR MEASURING AND ANALYZING RESIDENTIAL SEGREGATION. *Sociological Methodology*, 48(1), 182–224. <https://doi.org/10.1177/0081175018796871>
- Robinson. (2019, December 2). *The critical role of street lighting in London's smart city project*. NS Energy. <https://www.nsenenergybusiness.com/features/smart-city-street-lighting/>
- Robinson, L. (2023). *When Hackers Target Road Infrastructure: The Downside of*

- Smart Cars and Traffic Lights*. College of Information Studies. <https://ischool.umd.edu/news/when-hackers-target-road-infrastructure-the-downside-of-smart-cars-and-traffic-lights/>
- Rocha, A., Scheirer, W., Boulton, T., & Goldenstein, S. (2011). Vision of the unseen [Article]. *ACM Computing Surveys*, 43(4), 1–42. <https://doi.org/10.1145/1978802.1978805>
- Rondeau, M. B., Brantingham, P. L., & Brantingham, P. (2005). THE VALUE OF ENVIRONMENTAL CRIMINOLOGY FOR THE DESIGN PROFESSIONS OF ARCHITECTURE, URBAN DESIGN, LANDSCAPE ARCHITECTURE, AND PLANNING. In *Journal of Architectural and Planning Research* (Vol. 22). Winter.
- Ronen, E., & Shamir, A. (2016). Extended Functionality Attacks on IoT Devices: The Case of Smart Lights. *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, 3–12; 5. <https://doi.org/10.1109/EuroSP.2016.13>
- Roof, K., & Oleru, N. (2008). Public Health: Seattle and King County's Push for the Built Environment. *Journal of Environmental Health*, 71(1), 24–27. <https://search.proquest.com/docview/219710110?accountid=14511>
- Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & Mcquaid, R. (2015). *NIST Special Publication 800-160, Volume 2 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. <https://doi.org/10.6028/NIST.SP.800-160v2r1>
- Rosser, G., Davies, T., Bowers, K. J., Johnson, S. D., & Cheng, T. (2017). Predictive Crime Mapping: Arbitrary Grids or Street Networks? *J Quant Criminol*, 33, 569–594. <https://doi.org/10.1007/s10940-016-9321-x>
- Russon Mary-Ann. (2015, October 26). *Hackers turning millions of smart CCTV cameras into botnets for DDoS attacks*. Technology-Cybersecurity. <https://www.ibtimes.co.uk/hackers-turning-millions-smart-cctv-cameras-into-botnets-ddos-attacks-1525736>
- Ryabchikov, I., Teslya, N., & Druzhinin, N. (2020). Integrating Computer Vision Technologies for Smart Surveillance Purpose [Proceeding]. *2020 26th Conference of Open Innovations Association (FRUCT)*, 2020-(1), 392–401. <https://doi.org/10.23919/FRUCT48808.2020.9087479>
- S Chaudhari, B., & Zennaro, M. (2020). Security in low-power wide-area networks: state-of-the-art and development toward the 5G. In *LPWAN Technologies for IoT and M2M Applications* (pp. 373–396). Elsevier Science & Technology. <https://doi.org/10.1016/B978-0-12-818880-4.00018-1>
- S, F. (2019). UK FCA to ask banks to test resilience to cyberattacks, infrastructure failures - ProQuest. *SNL European Financials Daily*. <https://www.proquest.com/docview/2322956010?parentSessionId=F%2FUxvtHf o03MCvDFkox0bBbULB2PiJWmCNScdebaYJ8%3D&pq-origsite=primo&accountid=14511>
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors (Basel, Switzerland)*, 23(15), 6666. <https://doi.org/10.3390/s23156666>

- Salome, G., & Maassen, A. (2023). *Paris' Vision for a '15-Minute City' Sparks a Global Movement*. World Resources Institute. <https://www.wri.org/insights/paris-15-minute-city>
- Salvi, A., Spagnoletti, P., & Saad Noori, N. (2022). Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem. *Computers & Security*, 112, 102507. <https://doi.org/10.1016/j.cose.2021.102507>
- Sampson, R., Eck, J. E., & Dunham, J. (2010). Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure. *Security Journal*, 23(1), 37–51. <https://doi.org/10.1057/sj.2009.17>
- Sampson, R. J., Raudenbush, S. W., & Earls, F. (1997). Neighborhoods and Violent Crime: A Multilevel Study of Collective Efficacy. In *Source: Science, New Series* (Vol. 277, Issue 5328).
- Samuels, R. (2005). AFTER-DARK DESIGN, NIGHT ANIMATION, AND INTERPERSONAL INTERACTION: TOWARD A COMMUNITY-SECURITY PARADIGM. *Source: Journal of Architectural and Planning Research Journal of Architectural and Planning Research Journal of Architectural and Planning Research*, 22(224), 305–318. <http://www.jstor.org/stable/43030749>
- Sánchez, S. O. A., & Fuentes, F. C. M. (2016). The motor vehicle theft and its spatial relationship with the socio-demographic context in three Central Delegations of Mexico City (2010). *Investigaciones Geograficas*, 89(89), 107–120. <https://doi.org/10.14350/rig.48763>
- Sarieddine, K., Sayed, M. A., Torabi, S., Atallah, R., & Assi, C. (2023). Investigating the security of ev charging mobile applications as an attack surface. *ACM Transactions on Cyber-Physical Systems*, 7(4), 1–28.
- Sarieddine, K., Sayed, M. A., Torabi, S., Attallah, R., Jafarigiv, D., Assi, C., & Debbabi, M. (2024). *Uncovering Covert Attacks on EV Charging Infrastructure: How OCPP Backend Vulnerabilities Could Compromise Your System*.
- Saville, G., & Mihinjac, M. (2022). *Third-Generation CPTED—Integrating Crime Prevention and Neighbourhood Liveability BT - Urban Crime Prevention: Multi-disciplinary Approaches* (M. Saraiva (Ed.); pp. 27–54). Springer International Publishing. https://doi.org/10.1007/978-3-031-15108-8_2
- Savithramma, R. M., Ashwini, B. P., & Sumathi, R. (2022). *Smart Mobility Implementation in Smart Cities: A Comprehensive Review on State-of-art Technologies*. 10–17. <https://doi.org/10.1109/ICSSIT53264.2022.9716288>
- Say, M. (2023). *London leads smart lamppost project*. UK Authority News. <https://www.ukauthority.com/articles/london-leads-smart-lamppost-project/>
- Sayed, M., Atallah, R., Assi, C., & Debbabi, M. (2021). *Electric Vehicle Attack Impact on Power Grid Operation*.
- Schauer, S., Grafenauer, T., König, S., Warum, M., & Rass, S. (2019). Estimating cascading effects in cyber-physical critical infrastructures. *International Conference on Critical Information Infrastructures Security*, 43–56.
- Schmitz-Berndt, S., & Cole, M. D. (2022). Towards an Efficient and Coherent Regulatory Framework on Cybersecurity in the EU: The Proposals for a NIS 2.0

- Directive and a Cyber Resilience Act. *Applied Cybersecurity & Internet Governance*, 1(1), 1–17.
- Schneider, R. H. (2005). INTRODUCTION: CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (CPTED): THEMES, THEORIES, PRACTICE, AND CONFLICT. In *Source: Journal of Architectural and Planning Research* (Vol. 22, Issue 4). Winter. <https://www.jstor.org/stable/43030746>
- Schneier, B. (2015). *Secrets and Lies*. Wiley Publishing, Inc. <https://doi.org/10.1002/9781119183631>
- Schubert, H. (2016). Urban crime prevention – broadening of perspectives. *Journal of Place Management and Development*, 9(2), 120–136. <https://doi.org/10.1108/JPMD-09-2015-0031>
- Sharma, Rohit, & Arya, R. (2023). Security threats and measures in the Internet of Things for smart city infrastructure: A state of art. *Transactions on Emerging Telecommunications Technologies*, 34(11), e4571.
- Shaw, I. G. R. (2016). The Urbanization of drone warfare: policing surplus populations in the dronopolis. *Geogr. Helv*, 71, 19–28. <https://doi.org/10.5194/gh-71-19-2016>
- Shelden, D. (2018). Cyber-Physical Systems and the Built Environment. *Technology|Architecture + Design*, 2(2), 137–139. <https://doi.org/10.1080/24751448.2018.1497358>
- Sherman, L. W., Gartin, P. R., & Buerger, M. E. (1989). HOT SPOTS OF PREDATORY CRIME: ROUTINE ACTIVITIES AND THE CRIMINOLOGY OF PLACE*. *Criminology*, 27(1), 27–56. <https://doi.org/10.1111/j.1745-9125.1989.tb00862.x>
- Shukla, M. (2021, January 27). *Cyber resilience recommended actions*. Show & Tell Archives - LOTI. <https://youtu.be/0LLsRH5YrBM>
- Shukla, M., Johnson, S. D., & Jones, P. (2019, June 1). Does the NIS implementation strategy effectively address cyber security risks in the UK? *2019 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2019*. <https://doi.org/10.1109/CyberSecPODS.2019.8884963>
- Shuster, J. J. (2011). Review: Cochrane handbook for systematic reviews for interventions, Version 5.1.0, published 3/2011. Julian P.T. Higgins and Sally Green, Editors. *Research Synthesis Methods*, 2(2), 126–130. <https://doi.org/10.1002/jrsm.38>
- Skarga-Bandurova, I., Kotsiuba, I., & Biloborodova, T. (2022). Cyber security of electric vehicle charging infrastructure: Open issues and recommendations. *2022 IEEE International Conference on Big Data (Big Data)*, 3099–3106.
- Smart Cities World news team. (2023, February 17). *Mobility-as-a-Service - Liftango digitises West Midlands dial-a-ride service*. <https://www.smartcitiesworld.net/mobility-as-a-service/liftango-digitises-west-midlands-dial-a-ride-service-8663>
- SmartcitiesWorld news team. (2021). *Seoul begins roll-out of smart bus shelters*. Smartcitiesworld.Net News. <https://www.smartcitiesworld.net/news/seoul-begins-roll-out-of-smart-bus-shelters-6840>

- SmartCitiesWorld news team. (2023a, February 13). *Smart Cities World - Road travel - Partnership aims to streamline digital parking enforcement*. <https://www.smartcitiesworld.net/road-travel/partnership-aims-to-streamline-digital-parking-enforcement-8646>
- SmartCitiesWorld news team. (2023b, March 2). *Smart Cities World - Electric vehicles - Apcoa and BP Pulse to create European network of EV hubs*. <https://www.smartcitiesworld.net/electric-vehicles/apcoa-and-bp-pulse-to-create-european-network-of-ev-hubs-8708>
- Smith. (2018). *'I'm hacked' message left on dozens of defaced Canon IoT security cameras in Japan*. <https://www.csoonline.com/article/565354/im-hacked-message-left-on-dozens-of-defaced-canon-iot-security-cameras-in-japan.html>
- Smith, M. J. (2008). Addressing the Security Needs of Women Passengers on Public Transport. *Security Journal*, 21(21), 117–133. <https://doi.org/10.1057/palgrave.sj.8350071>
- Smith, T., & Stamatakis, N. (2020). Defining Cybercrime in Terms of Routine Activity and Spatial Distribution: Issues and Concerns. *International Journal of Cyber Criminology*, 14(2), 433–459. <https://doi.org/10.5281/zenodo.4769989>
- Sohn, D.-W. (2015). *Residential crimes and neighbourhood built environment: Assessing the effectiveness of crime prevention through environmental design (CPTED)*. <https://doi.org/10.1016/j.cities.2015.11.023>
- Somani, A., Sonpatki, S., Kasture, S., Kshirsagar, A., & Ali, N. R. Q. (2023). PAPER ON LIVE CRIMINAL DETECTION USING FACIAL RECOGNITION AND TRACKING ALGORITHMS. *International Research Journal of Modernization in Engineering Technology and Science*, 5(5). https://www.irjmets.com/uploadedfiles/paper/issue_5_may_2023/40429/final/fin_irjmets1685202854.pdf
- Soohyun O, Yongjei, L. (2016). Crime and land use in Pittsburgh: A micro-size grid-cell analysis of the influence of land-uses on area crime - ProQuest. *Crime Prevention and Community Safety*, 18(3), 204–227. https://search-proquest-com.libproxy.ucl.ac.uk/docview/1960539451?rfr_id=info%3Axri%2Fsid%3Aprimo#
- Soykan, E. U., Bagriyanik, M., & Soykan, G. (2021). Disrupting the power grid via EV charging: The impact of the SMS Phishing attacks. *Sustainable Energy, Grids and Networks*, 26, 100477.
- Staniforth, A. (2013). Securing Cyberspace. In *Strategic Intelligence Management* (pp. 213–223). Elsevier. <https://doi.org/10.1016/B978-0-12-407191-9.00017-X>
- Stats NZ. (2018). *Statistical standard for geographic areas*. <http://archive.stats.govt.nz/methods/classifications-and-standards/classification-related-stats-standards/geographic-areas/pg4.aspx>
- STeaPP. (2024). *Policy Brief: Strengthening cyber-resilience and procurement frameworks for connected places | UCL Department of Science, Technology, Engineering and Public Policy - UCL – University College London*. <https://www.ucl.ac.uk/steapp/policy-brief-strengthening-cyber-resilience-and-procurement-frameworks-connected-places>

- Steinbach, R., Perkins, C., & Thompson, L. (2015). The effect of reduced street lighting on road casualties and crime in England and Wales: controlled interrupted time series analysis. *J Epidemiol Community Health*, 69, 1118–1124. <https://doi.org/10.1136/jech>
- Steinbach, R., Perkins, C., Thompson, L., Johnson, S., Armstrong, B., Green, J., Grundy, C., Wilkinson, P., & Edwards, P. (2015). *The effect of reduced street lighting on road casualties and crime in England and Wales: controlled interrupted time series analysis*. [Article].
- Stellios, I., Mokos, K., & Kotzanikolaou, P. (2022a). Assessing smart light enabled cyber-physical attack paths on urban infrastructures and services [Article]. *Connection Science*, 34(1), 1401–1429. <https://doi.org/10.1080/09540091.2022.2072470>
- Stellios, I., Mokos, K., & Kotzanikolaou, P. (2022b). Assessing Vulnerabilities and IoT-Enabled Attacks on Smart Lighting Systems. In S. Katsikas, C. Lambrinoudakis, N. Cuppens, J. Mylopoulos, C. Kalloniatis, W. Meng, S. Furnell, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. Maestre Vidal, & M. A. Sotelo Monge (Eds.), *Computer Security. ESORICS 2021 International Workshops* (pp. 199–217). Springer International Publishing.
- Stitch World. (2019). USA: Amazon unveils its Scout delivery robots; to expand operations on the basis of test results. *Stitch World*.
- Šttilis, D., Pakutinskas, P., & Malinauskait, I. (2017). EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. *Security Journal*, 30(4), 1151–1168. <https://doi.org/10.1057/s41284-016-0083-9>
- Streetwise; Urban planning. (2015). *The Economist*, 416(8954), 63–64. https://ucl-new-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=TN_proquest1710030344&context=PC&vid=UCL_VU2&lang=en_US&search_scope=CSCOP_UCL&adaptor=primo_central_multiple_fe&tab=local&query=any,contains,urban streets redesign for pedestrian cyclist walking&offset=0
- Strupczewski, G. (2024). Mitigating Cyber Risk in Personal Finance of the Elderly. Insights into Vulnerabilities, Cyber Hygiene and the Role of Personal Cyber Insurance. *Cybersecurity and Law*, 11(1), 281–298.
- Stucky, T. D., & Smith, S. L. (2017). Exploring the conditional effects of bus stops on crime. *Security Journal*, 30(1), 290–309. <https://doi.org/10.1057/sj.2014.16>
- Stummvoll, G. (2012). Governance through norms and standards: The normative force behind design-led crime prevention. *Criminology & Criminal Justice*, 12(4), 377–396. <https://doi.org/10.1177/1748895812452280>
- Summers, L., & Johnson, S. D. (2017). Does the Configuration of the Street Network Influence Where Outdoor Serious Violence Takes Place? Using Space Syntax to Test Crime Pattern Theory. *Journal of Quantitative Criminology*, 33(2), 397–420. <https://doi.org/10.1007/s10940-016-9306-9>
- Sung-suk, V. Y., & Smith, M. J. (2014). Commuters using public transit in New York City: Using area-level data to identify neighbourhoods with vulnerable riders. *Security Journal*, 27, 194–209. <https://doi.org/10.1057/sj.2014.6>

- Sygensys. (2022). *Resilient Electrical Vehicle Charging: "REV" Work Package 1 report prepared by Sygensys for National Grid ESO*.
- Sygensys for National Grid ESO. (2022). *Resilient Electrical Vehicle Charging: "REV."* <https://esc-production-2021.s3.eu-west-2.amazonaws.com/2022/02/avNHxukq-Project-REV-WP1-report.pdf>
- Syrowatka, A., Kuznetsova, M., Alsubai, A., Beckman, A. L., Bain, P. A., Craig, K. J. T., Hu, J., Jackson, G. P., Rhee, K., & Bates, D. W. (2021). Leveraging artificial intelligence for pandemic preparedness and response: a scoping review to identify key use cases. *Npj Digital Medicine*, 4(1), 96. <https://doi.org/10.1038/s41746-021-00459-8>
- Tang, L., Lin, L., Shao, G., Su, X., & Zhao, J. (2011). Redefining the digital city for promoting sustainable urban development. *International Journal of Sustainable Development & World Ecology*, 18(6), 543–547. <https://doi.org/10.1080/13504509.2011.603762>
- Taylor, E., & Lee, M. (2019). Off the record?: Arrestee concerns about the manipulation, modification, and misrepresentation of police body-worn camera footage [Article]. *Surveillance & Society*, 17(3–4), 473–483. <https://doi.org/10.24908/ss.v17i3/4.6550>
- Taylor, RALPH B. (1997). Social Order and Disorder of Street Blocks and Neighborhoods: Ecology, Microecology, and the Systemic Model of Social Disorganization. *Journal of Research in Crime and Delinquency*, 34(1), 113–155. <https://doi.org/10.1177/0022427897034001006>
- Taylor, Ralph B, Haberman, C. P., & Groff, E. R. (2019). Urban park crime: Neighborhood context and park features. *Journal of Criminal Justice*, 64, 13–22. <https://doi.org/10.1016/j.jcrimjus.2019.101622>
- Tech Policy Press. (2020). *San Diego, Street Smarts and Surveillance*. Newsletter. <https://techpolicy.press/san-diego-street-smarts-and-surveillance/>
- Telep, C. W., Weisburd, D., Gill, C. E., Vitter, Z., & Teichman, D. (2014). Displacement of crime and diffusion of crime control benefits in large-scale geographic areas: a systematic review. *Journal of Experimental Criminology*, 10(4), 515–548. <https://doi.org/10.1007/S11292-014-9208-5>
- Telka, P. (2020). *Cops Tap Smart Streetlights Sparking Controversy and Legislation*. IEEE Spectrum. <https://spectrum.ieee.org/cops-smart-street-lights>
- Tenable Research. (2018). *Tenable Research Advisory: Peekaboo Critical Vulnerability in NUUO Network Video Recorder*. Tenable. <https://www.tenable.com/blog/tenable-research-advisory-peekaboo-critical-vulnerability-in-nuuo-network-video-recorder>
- Tessian Solutions. (2021). *What are Deepfakes? Are They a Security Threat?* ADVANCED EMAIL THREATS. <https://www.tessian.com/blog/what-are-deepfakes/>
- Thales. (2024). *IoT Cybersecurity: regulating the Internet of Things*. <https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/iot-regulations>

- The Byte. (2022). *Electric Vehicle Chargers Are Shockingly Vulnerable to Hacking*. <https://futurism.com/the-byte/ev-chargers-vulnerable-hacking>
- Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology*, 8(1), 1–10. <https://doi.org/10.1186/1471-2288-8-45/FIGURES/2>
- Toh, C. K. (2020). Security for smart cities [Article]. *IET Smart Cities*, 2(2), 95–104. <https://doi.org/10.1049/iet-smc.2020.0001>
- Toh, C. K., Sanguesa, J. A., Cano, J. C., & Martinez, F. J. (2020). Advances in smart roads for future smart cities. *Proceedings of the Royal Society A*, 476(2233). <https://doi.org/10.1098/RSPA.2019.0439>
- Tompson, L., Johnson, S., Ashby, M., Perkins, C., & Edwards, P. (2014). *Cartography and Geographic Information Science UK open source crime data: accuracy and possibilities for research UK open source crime data: accuracy and possibilities for research*. <https://doi.org/10.1080/15230406.2014.972456>
- Townsley, M., & Sidebottom, A. (2010). All offenders are equal, but some are more equal than others: Variation in journeys to crime between offenders [Article]. *Criminology*, 48(3), 897–917. <https://doi.org/10.1111/j.1745-9125.2010.00205.x>
- Transport and Environment. (2022). *Delivering a world-class charging network by 2030 A UK approach*. <https://www.zap-map.com/ev-market-statistics/>.
- Transport for London. (2017). *ACCESSIBLE BUS STOP DESIGN GUIDANCE*. <https://content.tfl.gov.uk/bus-stop-design-guidance.pdf>
- Transport For London. (2023). *Keeping London moving - Transport for London*. <https://tfl.gov.uk/>
- Transport Technology Forum. (2022). *Manual For Smart Streets - Smart streets Use case*. <https://mfss.ttf.uk.net/manual-for-smart-streets/smart-streets-use-cases/>
- Truntsevsky, Y. V., Lukiny, I. I., Sumachev, A. V., & Kopytova, A. V. (2018). A smart city is a safe city: The current status of street crime and its victim prevention using a digital application. *MATEC Web of Conferences*, 170. <https://doi.org/10.1051/mateconf/201817001067>
- Tu, M. (2022, August 25). *Here's What's Included in LA's New "High-Tech" Bus Shelters - dot.LA*. <https://dot.la/la-partner-tranzito-vector-2657943159.html>
- Tzezana, R. (2016). Scenarios for crime and terrorist attacks using the internet of things. *European Journal of Futures Research*, 4(1). <https://doi.org/10.1007/s40309-016-0107-z>
- U.S.Department of Energy, E. E. and R. E. (2022). *A Cybersecurity Threat Profile for a Connected Lighting System*. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-31958.pdf
- UK Cabinet Office. (2023). *Guidance: UK National Leadership for Risk Identification, Emergency Preparedness, Response and Recovery*. <https://www.gov.uk/government/publications/list-of-lead-government-departments-responsibilities-for-planning-response-and-recovery-from->

emergencies

- UK Government Legislation. (1998). *Crime and Disorder Act 1998*. The National Archives. <https://www.legislation.gov.uk/ukpga/1998/37/section/17>
- UK Police Crime Prevention Initiatives. (2024). *Internet of Things (IoT) Security*. <https://www.securedbydesign.com/internet-of-things>
- Uppal, M., Gupta, D., Goyal, N., Imoize, A. L., Kumar, A., Ojo, S., Pani, S. K., Kim, Y., & Choi, J. (2023). A Real-Time Data Monitoring Framework for Predictive Maintenance Based on the Internet of Things. *Complexity*, 2023, 9991029. <https://doi.org/10.1155/2023/9991029>
- Ursprung, R., & Gray, J. (2010). Random safety auditing, root cause analysis, failure mode and effects analysis. *Clinics in Perinatology*, 37(1), 141–165. <https://doi.org/10.1016/j.clp.2010.01.008>
- US-Congress.Gov. (2019). *H.R.1668 - IoT Cybersecurity Improvement Act of 2020*. <https://www.congress.gov/bill/116th-congress/house-bill/1668>
- Vaccari, C., & Chadwick, A. (2020). Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. *Social Media and Society*, 6(1). https://doi.org/10.1177/2056305120903408/SUPPL_FILE/DEEPFAKES_AND_DISINFORMATION_-_SUPPLEMENTARY_INFORMATION_FINAL.PDF
- Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the Adaptation of Routine Activity and Lifestyle Exposure Theories to Account for Cyber Abuse Victimization. *Journal of Contemporary Criminal Justice*, 32(2), 169–188. <https://doi.org/10.1177/1043986215621379>
- van Sleeuwen, S. E. M., Ruiter, S., & Menting, B. (2018). A time for a crime: temporal aspects of repeat offenders' crime location choices. *Journal of Research in Crime and Delinquency*, 55(4), 538–568.
- van Vliet, E., Dane, G., Weijs-Perrée, M., van Leeuwen, E., van Dinter, M., van den Berg, P., Borgers, A., & Chamilothoni, K. (2021). The Influence of Urban Park Attributes on User Preferences: Evaluation of Virtual Parks in an Online Stated-Choice Experiment. In *International Journal of Environmental Research and Public Health* (Vol. 18, Issue 1). <https://doi.org/10.3390/ijerph18010212>
- van Wilsem, J. (2011). 'Bought it, but Never Got it' Assessing Risk Factors for Online Consumer Fraud Victimization. *European Sociological Review*, 29(2), 168–178. <https://doi.org/10.1093/esr/jcr053>
- Vanberghen Cristina. (2022, December 28). *Ukraine marks a turning point for cyberwarfare – POLITICO*. <https://www.politico.eu/article/russia-ukraine-cyber-invasion-warfare-kremlin-nato/>
- Vandeviver, C., Van Daele, S., & Vander Beken, T. (2015). What Makes Long Crime Trips Worth Undertaking? Balancing Costs and Benefits in Burglars' Journey to Crime. *The British Journal of Criminology*, 55(2), 399–420. <https://doi.org/10.1093/bjc/azu078>
- Vennam, P., Pramod, T. C., Thippeswamy, B. M., Kim, Y.-G., & Pavan Kumar, B. N. (2021). Attacks and preventive measures on video surveillance systems: A review

- [Article]. *Applied Sciences*, 11(12), 5571. <https://doi.org/10.3390/app11125571>
- Vergouw, B., Nagel, H., Bondt, G., & Custers, B. (2016). *Drone Technology: Types, Payloads, Applications, Frequency Spectrum Issues and Future Developments*. 21–45. https://doi.org/10.1007/978-94-6265-132-6_2
- Vermesan, O., Bahr, R., Ottella, M., Serrano, M., Karlsen, T., Wahlstrøm, T., Sand, H. E., Ashwathnarayan, M., & Gamba, M. T. (2020). Internet of Robotic Things Intelligent Connectivity and Platforms. *Frontiers in Robotics and AI*, 7, 104. <https://doi.org/10.3389/FROBT.2020.00104/BIBTEX>
- Viegas, M. M. (2019). Smart Bus Stop: People Counting in a Multi-View Camera Environment [Universidade do Algarve (Portugal) PP - Portugal]. In *PQDT - Global*. <https://www.proquest.com/dissertations-theses/smart-bus-stop-people-counting-multi-view-camera/docview/2674875183/se-2?accountid=14511>
- Vilalta, C. J., & Fondevila, G. (2019). Modeling Crime in an Uptown Neighborhood: The Case of Santa Fe in Mexico City. *Papers in Applied Geography*, 5(1–2), 1–12. <https://doi.org/10.1080/23754931.2018.1554502>
- Virta, S. (2013). Governing urban security in Finland: Towards the ‘European model.’ *European Journal of Criminology*, 10(3), 341–353. <https://doi.org/10.1177/1477370812473536>
- Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security*, 83, 313–331. <https://doi.org/10.1016/J.COSE.2019.02.009>
- Vogiatzaki, M., Zerefos, S., & Tania, M. H. (2020). Enhancing city sustainability through smart technologies: A framework for automatic pre-emptive action to promote safety and security using lighting and ICT-based surveillance. *Sustainability*, 12(15), 6142. <https://doi.org/10.3390/su12156142>
- Walters, D. (2011). Smart cities, smart places, smart democracy: Form-based codes, electronic governance and the role of place in making smart cities [Article]. *Intelligent Buildings International* (London), 3(3), 198–218. <https://doi.org/10.1080/17508975.2011.586670>
- Wang, S.-Y. K., & Hsieh, M.-L. (2021). The ATM Hacking Case. In *Digital Robbery: ATM Hacking and Implications* (pp. 15–32). Springer International Publishing. https://doi.org/10.1007/978-3-030-70706-4_3
- Wang, Z., & Li, Y. (2022). Could social media reflect acquisitive crime patterns in London? *Journal of Safety Science and Resilience*, 3(2), 115–127. <https://doi.org/https://doi.org/10.1016/j.jnlssr.2021.08.007>
- Webb, R., Bai, X., Smith, M. S., Costanza, R., Griggs, D., Moglia, M., Neuman, M., Newman, P., Newton, P., Norman, B., Ryan, C., Schandl, H., Steffen, W., Tapper, N., & Thomson, G. (2018). Sustainable urban systems: Co-design and framing for transformation. *Ambio*, 47(1), 57–77. <https://doi.org/10.1007/s13280-017-0934-6>
- Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review: The International Journal of*

- Wei, F., & Lin, X. (2023). Cyber-Physical Attack Launched from EVSE Botnet. *IEEE Transactions on Power Systems*.
- Weinert, J. (2019). *For smart street lighting security, think authentication*. Signify. <https://www.signify.com/en-us/blog/archive/smart-city/importance-of-security-and-data-privacy-for-smart-street-lighting>
- Weisburd, D. (2015). The Law and Crime Concentration and the Criminology of Place. *Criminology*, 53. <https://heinonline.org/HOL/Page?handle=hein.journals/crim53&id=149&div=15&collection=journals>
- Weisburd, D., Bernasco, W., & Bruinsma, G. J. N. (2009). Putting crime in its place: Units of analysis in geographic criminology. In *Putting Crime in its Place: Units of Analysis in Geographic Criminology*. Springer New York. <https://doi.org/10.1007/978-0-387-09688-9>
- Weisburd, D., Eck, J. E., Braga, A. A., Telep, C. W., Cave, B., Bowers, K., Bruinsma, G., Gill, C., Groff, E., Hibdon, J., Hinkle, J. C., Johnson, S. D., Lawton, B., Lum, C., Ratcliffe, J., Rengert, G., Taniguchi, T., & Yang, S.-M. (2016a). The Concentration of Crime at Place. In *Place Matters* (pp. 16–41). Cambridge University Press. <https://doi.org/10.1017/CBO9781139342087.003>
- Weisburd, D., Eck, J. E., Braga, A. A., Telep, C. W., Cave, B., Bowers, K., Bruinsma, G., Gill, C., Groff, E., Hibdon, J., Hinkle, J. C., Johnson, S. D., Lawton, B., Lum, C., Ratcliffe, J., Rengert, G., Taniguchi, T., & Yang, S.-M. (2016b). Theories of Crime and Place. In *Place Matters* (pp. 42–67). Cambridge University Press. <https://doi.org/10.1017/CBO9781139342087.004>
- Weisburd, D., Groff, E. (Elizabeth R.), & Yang, S.-M. (2012). *The criminology of place : street segments and our understanding of the crime problem*. Oxford University Press.
- Weisburd, D., Wyckoff, L. A., Ready, J., Eck, J. E., Hinkle, J. C., & Gajewski, F. (2006). Does crime just move around the corner? A controlled study of spatial displacement and diffusion of crime control benefits. *Criminology*, 44(3), 549–592. <https://doi.org/10.1111/J.1745-9125.2006.00057.X>
- Welsh, B. C., Rocque, M., Welsh, B. C., & Rocque, M. (2014). When crime prevention harms: a review of systematic reviews. *J Exp Criminol*, 10, 245–266. <https://doi.org/10.1007/s11292-014-9199-2>
- Welsh, B. C., & Taheri, S. A. (2018). *What Have We Learned from Environmental Criminology for the Prevention of Crime?* (G. J. N. Bruinsma & S. D. Johnson (Eds.); Vol. 1). Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780190279707.013.31>
- Westminster City Council. (2013). *Parking Technology-Westminster City Council*.
- Wheeler, A. P. (2016). Quantifying the local and spatial effects of alcohol outlets on crime. *Crime Delinq*. <https://doi.org/10.2139/ssrn.2869198>
- Whitmore, W. (2020). *EVOLVING RANSOMWARE TESTS BANKS' RESILIENCE*

Cyber risk - ProQuest. Business Today.
<https://www.proquest.com/docview/2439612887/fulltext/8BC69ACDA57641C5PQ/1?accountid=14511>

- Wielicka-Gańczarczyk, K., & Jonek-Kowalska, I. (2023). Perceptions and Attitudes toward Risks of City Administration Employees in the Context of Smart City Management [Article]. *Smart Cities*, 6(3), 1325–1344. <https://doi.org/10.3390/smartcities6030064>
- Wilkinson, S. (1998). Focus group methodology: a review [Article]. *International Journal of Social Research Methodology*, 1(3), 181–203. <https://doi.org/10.1080/13645579.1998.10846874>
- Williams, M. L., Edwards, A., Housley, W., Burnap, P., Rana, O., Avis, N., Morgan, J., & Sloan, L. (2013). Policing cyber-neighbourhoods: tension monitoring and social media networks. *Policing and Society*, 23(4), 461–481. <https://doi.org/10.1080/10439463.2013.780225>
- Wo, J. C., & Park, J. (2020). An Examination of Schools, Social Ecological Factors, and Neighbourhood Crime. *British Journal of Criminology*, 60(4), 851–872. <https://doi.org/10.1093/bjc/azaa002>
- Wolbertus, R., Jansen, S., & Kroesen, M. (2020). Stakeholders' perspectives on future electric vehicle charging infrastructure developments [Article]. *Futures: The Journal of Policy, Planning and Futures Studies*, 123, 102610. <https://doi.org/10.1016/j.futures.2020.102610>
- Wolf, K., Dawson, R. J., Mills, J. P., Blythe, P., & Morley, J. (2022). Towards a digital twin for supporting multi-agency incident management in a smart city [Article]. *Scientific Reports*, 12(1), 16221–16221. <https://doi.org/10.1038/s41598-022-20178-8>
- World Economic Forum. (2016). *Understanding Systemic cyber risk*. <https://www.zurich.com/-/media/project/zurich/dotcom/industry-knowledge/cyber-risk/docs/wef-report-understanding-systemic-cyber-risk-oct-2016.pdf>
- Wortley, R., & Townsley, M. (2016). *Environmental Criminology and Crime Analysis*. Taylor & Francis. <https://books.google.co.uk/books?id=uzQIDwAAQBAJ>
- Wortley, Richard, & Mazerolle, L. G. (2008). *Environmental criminology and crime analysis / edited by Richard Wortley and Lorraine Mazerolle*. Cullompton, Devon : Willan.
- WPI Economics. (2021). *OUTLINING A UK VISION FOR 2030*. <https://www.wwf.org.uk/sites/default/files/2021-10/Outlining-UK-Vision-for-2030.pdf>
- Wu, Y., & Ridgeway, G. (2021). Effect of public transit on crime: evidence from SEPTA strikes in Philadelphia. *Journal of Experimental Criminology*, 17(2), 267–286. <https://doi.org/10.1007/s11292-020-09416-z>
- Wuschke, K., & Kinney, J. B. (2018). *Built Environment, Land Use, and Crime* (G. J. N. Bruinsma & S. D. Johnson (Eds.); Vol. 1). Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780190279707.013.14>

- Wyss, G. D., Sholander, P. E., Darby, J. L., & Phelan, J. M. (2007). *Identifying and Defeating Blended Cyber-Physical Security Threats*.
- Xie, H., Liu, L., & Yue, H. (2022). Modeling the Effect of Streetscape Environment on Crime Using Street View Images and Interpretable Machine-Learning Technique. In *International Journal of Environmental Research and Public Health* (Vol. 19, Issue 21). <https://doi.org/10.3390/ijerph192113833>
- Xu, H., & Geng, X. (2019). People-Centric Service Intelligence for Smart Cities. In *Smart Cities* (Vol. 2, Issue 2, pp. 135–152). <https://doi.org/10.3390/smartcities2020010>
- Xu, Y., Fu, C., Kennedy, E., Jiang, S., & Owusu-Agyemang, S. (2018). The impact of street lights on spatial-temporal patterns of crime in Detroit, Michigan. *Cities*, 79, 45–52. <https://doi.org/10.1016/j.cities.2018.02.021>
- Yaacoub, J. P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things*, 11, 100218. <https://doi.org/10.1016/J.IOT.2020.100218>
- Yang, L., Sahlqvist, S., McMinn, A., Griffin, S. J., & Ogilvie, D. (2010). Interventions to promote cycling: Systematic review. In *BMJ (Online)* (Vol. 341, Issue 7778, p. 870). <https://doi.org/10.1136/bmj.c5293>
- Yar, M. (2012). E-Crime 2.0: the criminological landscape of new social media. *Information & Communications Technology Law*, 21(3), 207–219. <https://doi.org/10.1080/13600834.2012.744224>
- Yasin, A., Fatima, R., Wen, L., Afzal, W., Azhar, M., & Torkar, R. (2020). On Using Grey Literature and Google Scholar in Systematic Literature Reviews in Software Engineering. *IEEE Access*, 8, 36226–36243. <https://doi.org/10.1109/ACCESS.2020.2971712>
- Yilmaz, Y., & Uludag, S. (2021). Timely detection and mitigation of IoT-based cyberattacks in the smart grid [Article]. *Journal of the Franklin Institute*, 358(1), 172–192. <https://doi.org/10.1016/j.jfranklin.2019.02.011>
- Yoon, Y.-I., & Chun, J.-A. (2014). Tracking system for mobile user based on CCTV [Proceeding]. *International Conference on Information Networking*, 374–378. <https://doi.org/10.1109/ICOIN.2014.6799708>
- Yorio, Z., Oram, R., El-Tawab, S., Salman, A., Heydari, M. H., & Park, B. B. (2018). Data analysis and information security of an Internet of Things (IoT) intelligent transit system. *2018 Systems and Information Engineering Design Symposium (SIEDS)*, 24–29. <https://doi.org/10.1109/SIEDS.2018.8374744>
- Yunos, Z., & Hafidz Suid, S. (2010). Protection of Critical National Information Infrastructure (CNII) against cyber terrorism: Development of strategy and policy framework. *2010 IEEE International Conference on Intelligence and Security Informatics*, 169–169. <https://doi.org/10.1109/ISI.2010.5484748>
- Zaharia, G. C., Zaharia, C., Tudorescu, N., & Zaharia, I. (2010). ONLINE CRIME AND THE REGULATION OF BUSINESS ON THE INTERNET. *Economics, Management and Financial Markets*, 5(4), 238–243. https://search-proquest-com.libproxy.ucl.ac.uk/docview/857667366?rfr_id=info%3Axri%2Fsid%3Aprimo

- Zahnow, R., & Corcoran, J. (2019). Crime and bus stops: An examination using transit smart card and crime data. *Environment and Planning B: Urban Analytics and City Science*, 239980831989061. <https://doi.org/10.1177/2399808319890614>
- Zenzic. (2022). *CAM Roadmap - Zenzic*. <https://zenzic.io/insights/roadmap/>
- Zhang, H., Zhao, S., Liu, R., Wang, W., Hong, Y., & Hu, R. (2022). Automatic Traffic Anomaly Detection on the Road Network with Spatial-Temporal Graph Neural Network Representation Learning. *Wireless Communications and Mobile Computing*, 2022, 4222827. <https://doi.org/10.1155/2022/4222827>
- Zhang, S., Leidner, D., Cao, X., & Liu, N. (2022). Workplace cyberbullying: A criminological and routine activity perspective. *Journal of Information Technology*, 37(1), 51–79. <https://doi.org/10.1177/02683962211027888>
- Zhang, T., Ji, X., Zhuang, Z., & Xu, W. (2019). JamCatcher: A Mobile Jammer Localization Scheme for Advanced Metering Infrastructure in Smart Grid. *Sensors (Basel, Switzerland)*, 19(4). <https://doi.org/10.3390/S19040909>
- Zhang, X., & Chen, P. (2023). The Impact of Urban Facilities on Crime during the Pre- and Pandemic Periods: A Practical Study in Beijing. *International Journal of Environmental Research and Public Health*, 20(3), 2163. <https://doi.org/10.3390/ijerph20032163>
- Zhao, R., John, S., Karas, S., Bussell, C., Roberts, J., Six, D., Gavett, B., & Yue, C. (2017). Design and evaluation of the highly insidious extreme phishing attacks. *Computers & Security*, 70, 634–647. <https://doi.org/10.1016/J.COSE.2017.08.008>
- Zhon, H., & Asiamah, A. A. (2022). The Prevalence and Mechanisms of cyber fraud activities among Ghanaian Youths; Routine Activity, Space Transition, and Rational Choice from Differential Association Perspective. *ISTAS*, 1, 1–7. <https://doi.org/10.1109/ISTAS55053.2022.10227127>
- Zhu, L., Gorman, D. M., & Horel, S. (2004). Alcohol outlet density and violence: A geospatial analysis. *Alcohol And Alcoholism*, 39(4), 369–375.
- Zukis Bob. (2021, September 2). *Some Vital Lessons In How Systemic Risk Is Changing Cybersecurity*. Forbes. <https://www.forbes.com/sites/bobzukis/2021/09/02/some-vital-lessons-in-how-systemic-risk-is-changing-cybersecurity/>
- Zurich Insurance. (2018, March 5). *Intensifying systemic risks are a growing threat to global progress | Zurich Insurance*. Digital, Data & Cyber. <https://www.zurich.com/en/knowledge/topics/digital-data-and-cyber/intensifying-systemic-risks-are-a-growing-threat-to-global-progress>
- Zurich Resilience Solutions. (2021). *Risk Insight: Electric Vehicle Charging*. <https://www.zurich.co.uk/-/media/news-and-insight/documents/useful-documents/zrs-ev-charging.pdf>

Appendix 1

Search keywords for systematic literature review in Chapter 3

1. Filter A

Filter A. Elements of Street design and urban planning Keywords within each column are connected by "OR" connector. Search results of each column are connected by "OR" connector.			
Keywords for Urban physical environment	Keywords for street elements	Keywords for urban design elements	Keywords for generic smart city elements
"Built environment"	"street" in same sentence as "tree*" within 5 words	"neighborhood" OR "neighbourhood" in same sentence as "design" within 5 words	"Smart city"
"neighborhood" OR "neighbourhood"	"street" in same sentence as "green" within 5 words	"urban" in same sentence as "design" within 2 words	"Smart street"
"Physical environment"	"street" in same sentence as "furniture" within 5 words	"building" in same sentence as "design" within 5 words	"drone"
"Urban place"	"micro" in same sentence as "facilit*" within 5 words	"urban" in same sentence as "planning" within 2 words	"wifi"
"urban" in same sentence as "space" within 5 words	"urban" in same sentence as "facilit*" within 5 words	"Land use"	"Smart phone"
"urban" in same sentence as "area" within 5 words	"super" in same sentence as "facilit*" within 5 words	"street" in same sentence as "design" within 2 words	"smart" in same sentence as "transport" within 5 words
"public" in same sentence as "realm" within 5 words	"street" in same sentence as "facilit*" within 5 words	"crime" in same sentence as "streetlight" within 5 words	"Mobile phone"
"micro*" in same sentence as "place" within 5 words	"urban" in same sentence as "transport*" within 5 words	"Crime generat**"	"Cell phone"
"street*" in same sentence as "urban" within 2 words	"street" in same sentence as "transport*" within 5 words	"Crime attract**"	"building" in same sentence as "sensor" within 5 words
"street" in same sentence as "network" within 5 words	"street" in same sentence as "transit*" within 5 words		"IoT" in same sentence as "device" within 5 words
"road" in same sentence as "network" within 5 words	"road" in same sentence as "transport*" within 5 words		"IoT" in same sentence as "urban" within 5 words
"Street segment"	"rail*" in same sentence as "station*" within 2 words		"Big data"
"Street configuration"	"bus*" in same sentence as "station*" within 2 words		"cyber"
"street" in same sentence as "ecosystem" within 5 words	"bus" in same sentence as "stop*" within 2 words		"virtual"
"street" in same sentence as "traffic" within 5 words	"park**"		
"street" in same sentence as "one-way" within 5 words	"underground" in same sentence as "rail" within 5 words		
"street" in same sentence as "two-way" within 5 words	"underground" in same sentence as "station" within 5 words		
	"underground" in same sentence as "transit*" within 5 words		
	"street" in same sentence as "walk*" within 5 words		
	"street" in same sentence as "pedestrian*" within 5 words		
	"street" in same sentence as "freight*" within 5 words		

2. Filter B

Filter B. Crime patterns and Impacts Keywords within each column are connected by "OR" connector. Search results of each column are connected by "AND" connector	
Keywords for changes to crime	Keywords for crime analysis
"crime" in same sentence as "influ*" within 5 words	"crime" in same sentence as "correlation" within 5 words
"crime" in same sentence as "impact*" within 2 words	"crime" in same sentence as "spati*" within 5 words
"crime" in same sentence as "affect*" within 2 words	"crime" in same sentence as "tempo*" within 5 words
"crime" in same sentence as "risk*" within 5 words	"crime" in same sentence as "spatiotemporal" within 5 words
"crime" in same sentence as "distribut*" within 5 words	"Crime pattern"
	"crime" in same sentence as "predict*" within 5 words
	"crime" in same sentence as "GIS" within 5 words
	"crime" in same sentence as "forecast*" within 5 words

3. Filter C

Filter C. Crime types	
Keywords within each column are connected by "OR" connector. Search results of each column are connected by "AND" connector	
Keywords for physical crimes	Keywords for cyber crimes / security
"abduct*"	"cyber" in same sentence as "crime" within 5 words
"arson"	"cyber" in same sentence as "fraud" within 5 words
"Assault"	"cyber" in same sentence as "security" within 5 words
"blackmail"	"cyber" in same sentence as "abuse" within 5 words
"bodily harm"	"cyber" in same sentence as "stalk*" within 5 words
"burglar*"	"Digi*" in same sentence as "security" within 5 words
"firearm"	"Digi*" in same sentence as "intervention" within 5 words
"weapon"	"DDOS"
"fraud"	"Ransom*"
"homicide"	
"kidnapping"	
"manslaughter"	
"murder"	
"prostitut*"	
"Public disorder"	
"robber*"	
"shoot*"	
"shoplift*"	
"theft"	
"vandalism"	
"violen*"	
"terrori*"	
"rape"	
"riot"	
"anti*social" in same sentence as "behavior*" within 2 words	
"knife" in same sentence as "crim*" within 2 words	
"money" in same sentence as "laundering" within 2 words	
"drug" in same sentence as "misuse" within 2 words	
"drug" in same sentence as "use" within 2 words	
"drug" in same sentence as "posse*" within 2 words	
"drug" in same sentence as "deal*" within 2 words	

4. Filter D

Filter D. Quantitative Analysis Keywords within each column are connected by "OR" connector.	
Keywords for Quantitative analysis	
"coefficient"	
"regression*"	
"quantitative" in same sentence as "analysis" within 2 words	
"analysis" in same sentence as "regression" within 5 words	
"econometric" in same sentence as "analyses" within 2 words	

NOTE: "*" indicates a wildcard, so that (for example) " redu*" would identify "reduce", "reducing", "reduction" and so on.

5. The search strings used based on the identified keywords

ProQuest:

("built environment") OR (neighbourhood*) OR ("neighbourhood*") OR ("physical environment") OR ("urban place") OR (urban NEAR/5 space) OR (urban NEAR/5 area*) OR (public NEAR/5 realm) OR (micro* NEAR/5 place) OR (street NEAR/2 urban) OR (street NEAR/2 Network) OR (road NEAR/2 network) OR ("Street Segment") OR ("Street configuration") OR (street NEAR/5 ecosystem) OR (street NEAR/5 traffic) OR (street NEAR/5 one-way) OR (Street NEAR/5 Two-way)

OR (street NEAR/5 tree) OR (street NEAR/5 green) OR (street NEAR/5 furniture) OR (micro NEAR/5 facilit*) OR (urban NEAR/2 facilit*) OR (super NEAR/5 facilit*) OR (street NEAR/5 facilit*) OR (urban NEAR/5 transport*) OR (Street NEAR/5 Transport*) OR (Street NEAR/5 Transit*) OR (road NEAR/5 transport*) OR (rail* NEAR/2 Station*) OR (bus NEAR/2 Station*) OR (bus NEAR/2 stop*) OR (park*) OR (underground NEAR/5 rail) OR (underground NEAR/5 station) OR (station NEAR/5 Transit*) OR (system NEAR/5 Transit*) OR (street NEAR/5 walk*) OR (street NEAR/5 pedestrian*) OR (street NEAR/5 freight*)

OR (Neighborhood* NEAR/5 design) OR (Neighbourhood* NEAR/5 design) OR (urban NEAR/2 design) OR (building NEAR/5 design) OR (urban NEAR/2 planning) OR ("land use") OR (street NEAR/2 design) OR (CRIME NEAR/5 "street light*") OR (intervention NEAR/5 "street light*") OR (intervention NEAR/5 CCTV) OR (crime NEAR/5 CCTV) OR ("crime generat*") OR ("crime attract*")

OR ("smart city") OR ("smart street") OR (drone) OR (wifi) OR ("smart phone") OR (smart NEAR/5 transport) OR ("mobile Phone") OR ("cell phone") OR (building NEAR/5 sensor*) OR (IoT NEAR/5 device) OR (IoT NEAR/5 urban) OR ("big data") OR ("cyber") OR ("virtual")

AND (influ* NEAR/5 crime) OR (crime NEAR/5 correlation) OR (crime NEAR/5 spati*) OR (crime NEAR/5 tempo*) OR (crime NEAR/5 spatiotemporal) OR ("crime pattern*") OR (Crime NEAR/5 predict*) OR (Crime NEAR/5 forecast*) OR (crime NEAR/2 impact*) OR (crime NEAR/2 affect*) OR (Crime NEAR/2 risk*) OR (Crime NEAR/5 GIS) OR (Distribut* NEAR/5 crime)

AND (coefficient) OR (Regression*) OR (quantitative* NEAR/2 Analysis) OR (analysis* NEAR/5 regression) OR (econometric NEAR/2 analyses)

AND ((abduct*) OR (arson*) OR (assault*) OR (blackmail) OR ("bodily harm") OR (burglar*) OR (firearm) OR (weapon) OR (fraud) OR (homicide) OR (kidnapping) OR (manslaughter) OR (murder) OR (prostitut*) OR ("public disorder") OR (robber*) OR (shoot*) OR (shoplift*) OR (theft*) OR (vandalism) OR (violen*) OR (terrori*) OR (rape) OR (riot*) OR (anti*social NEAR/2 behavio*) OR (knife NEAR/2 crim*) OR (money NEAR/2 laundering) OR (drug NEAR/2 misuse) OR (drug NEAR/2 use) OR (drug NEAR/2 possess*) OR (drug NEAR/2 deal*) OR (drug NEAR/2 traffick*) OR (drug NEAR/2 supply) OR (drug NEAR/2 market) OR (drug NEAR/2 abuse) OR (cyber NEAR/5 crime) OR (cyber NEAR/5 fraud) OR (cyber NEAR/5 security) OR (cyber NEAR/5 abuse) OR (Cyber NEAR/5 stalk*) OR (Digi* NEAR/5 security) OR (digi NEAR/5 intervention) OR (DDOS) OR (Ransom*))

Scopus:

((TITLE-ABS-KEY("built environment") OR TITLE-ABS-KEY(neighbourhood*) OR (neighbourhood*) OR TITLE-ABS-KEY("physical environment") OR TITLE-ABS-KEY("urban place") OR TITLE-ABS-KEY(urban W/5 space) OR TITLE-ABS-KEY(urban W/5 area*) OR TITLE-ABS-KEY(public W/5 realm) OR TITLE-ABS-KEY(micro* W/5 place) OR TITLE-ABS-KEY(street W/2 urban) OR TITLE-ABS-KEY(street W/2 Network) OR TITLE-ABS-KEY(road W/2 network) OR TITLE-ABS-KEY("Street Segment") OR TITLE-ABS-KEY("Street configuration") OR TITLE-ABS-KEY(street W/5 ecosystem) OR TITLE-ABS-KEY(street W/5 traffic) OR TITLE-ABS-KEY(street W/5 one-way) OR TITLE-ABS-KEY(Street W/5 Two-way) OR TITLE-ABS-KEY(street W/5 tree) OR TITLE-ABS-KEY(street W/5 green) OR TITLE-ABS-KEY(street W/5 furniture) OR TITLE-ABS-KEY(micro W/5 facilit*) OR TITLE-ABS-KEY(urban W/2 facilit*) OR TITLE-ABS-KEY(super W/5 facilit*) OR TITLE-ABS-KEY(street W/5 facilit*) OR TITLE-ABS-KEY(urban W/5 transport) OR TITLE-ABS-KEY(Street W/5 Transport*) OR TITLE-ABS-KEY(Street W/5 Transit*) OR TITLE-ABS-KEY(road W/5 transport) OR TITLE-ABS-KEY(rail* W/2 Station*) OR TITLE-ABS-KEY(bus W/2 Station*) OR TITLE-ABS-KEY(bus W/2 stop*) OR TITLE-ABS-KEY(park*) OR TITLE-ABS-KEY(underground W/5 rail) OR TITLE-ABS-KEY(underground W/5 station) OR TITLE-ABS-KEY(station W/5 Transit*) OR TITLE-ABS-KEY(system W/5 Transit*) OR TITLE-ABS-KEY(street W/5 walk*) OR TITLE-ABS-KEY(street W/5 pedestrian*) OR TITLE-ABS-KEY(street W/5 freight*) OR TITLE-ABS-KEY(Neighborhood* W/5 design) OR TITLE-ABS-KEY(Neighbourhood* W/5 design) OR TITLE-ABS-KEY(urban W/2 design) OR TITLE-ABS-KEY(building W/5 design) OR TITLE-ABS-KEY(urban W/2 planning) OR TITLE-ABS-KEY("land use") OR TITLE-ABS-KEY(street W/2 design) OR TITLE-ABS-KEY(CRIME W/5 "street light*") OR TITLE-ABS-KEY(intervention W/5 "street light*") OR TITLE-ABS-KEY(intervention W/5 CCTV) OR TITLE-ABS-KEY(crime W/5 CCTV) OR TITLE-ABS-KEY("crime generat*") OR TITLE-ABS-KEY("crime attract*") OR TITLE-ABS-KEY("smart city") OR TITLE-ABS-KEY("smart street") OR TITLE-ABS-KEY(smart W/5 transport) OR TITLE-ABS-KEY(drone) OR TITLE-ABS-KEY(wifi) OR TITLE-ABS-KEY("smart phone") OR TITLE-ABS-KEY("mobile Phone") OR TITLE-ABS-KEY("cell phone") OR TITLE-ABS-KEY(building W/5 sensor*) OR TITLE-ABS-KEY(IoT W/5 device) OR TITLE-ABS-KEY(IoT W/5 urban) OR TITLE-ABS-KEY("big data") OR TITLE-ABS-KEY("cyber") OR TITLE-ABS-KEY("virtual")) AND (TITLE-ABS-KEY (influ* W/5 crime) OR TITLE-ABS-KEY(crime W/5 correlation) OR TITLE-ABS-KEY(crime W/5 spati*) OR TITLE-ABS-KEY(crime W/5 tempo*) OR TITLE-ABS-KEY(crime W/5 spatiotemporal) OR TITLE-ABS-KEY("crime pattern*") OR TITLE-ABS-KEY(Crime W/5 predict*) OR TITLE-ABS-KEY(Crime W/5 forecast*) OR TITLE-ABS-KEY(crime W/2 impact*) OR TITLE-ABS-KEY(crime W/2 affect*) OR TITLE-ABS-KEY(Crime W/2 risk*) OR TITLE-ABS-KEY(Crime W/5 GIS) OR TITLE-ABS-KEY(Distribut* W/5 crime)) AND (TITLE-ABS-KEY (coefficient) OR TITLE-ABS-KEY(Regression*) OR TITLE-ABS-KEY(quantitative* W/2 Analysis) OR TITLE-ABS-KEY(analysis* W/5 regression) OR TITLE-ABS-KEY (econometric W/2 analyses)) AND (TITLE-ABS-KEY(abduct*) OR TITLE-ABS-KEY(arson*) OR TITLE-ABS-KEY(assault*) OR TITLE-ABS-KEY(blackmail) OR TITLE-ABS-KEY("bodily harm") OR TITLE-ABS-KEY(burglar*) OR TITLE-ABS-KEY(firearm) OR TITLE-ABS-KEY(weapon) OR TITLE-ABS-KEY(fraud) OR TITLE-ABS-KEY(homicide) OR TITLE-ABS-KEY(kidnapping) OR TITLE-ABS-KEY(manslaughter) OR TITLE-ABS-KEY(murder) OR TITLE-ABS-KEY(prostitut*) OR TITLE-ABS-KEY("public disorder") OR TITLE-ABS-KEY(robber*) OR TITLE-ABS-KEY(shoot*) OR TITLE-ABS-KEY(shoplift*) OR TITLE-ABS-KEY(theft*) OR TITLE-ABS-KEY(vandalism) OR TITLE-ABS-KEY(violen*) OR TITLE-ABS-KEY(terrori*) OR TITLE-ABS-KEY(rape) OR TITLE-ABS-KEY(riot*) OR TITLE-ABS-KEY(anti*social W/2 behavio*) OR TITLE-ABS-KEY(knife W/2 crim*) OR TITLE-ABS-KEY(money W/2 laundering) OR TITLE-ABS-KEY(drug W/2 misuse) OR TITLE-ABS-KEY(drug W/2 use) OR TITLE-ABS-KEY(drug W/2 possess*) OR TITLE-ABS-KEY(drug W/2 deal*) OR TITLE-ABS-KEY(drug W/2 traffick*) OR TITLE-ABS-KEY(drug W/2 supply) OR TITLE-ABS-KEY(drug W/2 market) OR TITLE-ABS-KEY(drug W/2 abuse) OR TITLE-ABS-KEY(cyber W/5 crime) OR TITLE-ABS-KEY(cyber W/5 fraud) OR TITLE-ABS-KEY(cyber W/5 security) OR TITLE-ABS-KEY(cyber W/5 abuse) OR TITLE-ABS-KEY(Cyber W/5 stalk*) OR TITLE-ABS-KEY(Digi* W/5 security) OR TITLE-ABS-KEY(digi W/5 intervention) OR TITLE-ABS-KEY(DDOS)OR TITLE-ABS-KEY(Ransom)))

OR ((TITLE-ABS-KEY("built environment") OR TITLE-ABS-KEY(neighborhood*) OR TITLE-ABS-KEY(neighbourhood*) OR TITLE-ABS-KEY("physical environment") OR TITLE-ABS-KEY("urban place") OR TITLE-ABS-KEY(urban W/5 space) OR TITLE-ABS-KEY(urban W/5 area*) OR TITLE-ABS-KEY(public W/5 realm) OR TITLE-ABS-KEY(micro* W/5 place) OR TITLE-ABS-KEY(street W/2 urban) OR TITLE-ABS-KEY(street W/2 Network) OR TITLE-ABS-KEY(road W/2 network) OR TITLE-ABS-KEY("Street Segment") OR TITLE-ABS-KEY("Street configuration") OR TITLE-ABS-KEY(street W/5 ecosystem) OR TITLE-ABS-KEY(street W/5 traffic) OR TITLE-ABS-KEY(street W/5 one-way) OR TITLE-ABS-KEY(Street W/5 Two-way) OR TITLE-ABS-KEY(street W/5 tree) OR TITLE-ABS-KEY(street W/5 green) OR TITLE-ABS-KEY(street W/5 furniture) OR TITLE-ABS-KEY(micro W/5 facilit*) OR TITLE-ABS-KEY(urban W/2 facilit*) OR TITLE-ABS-KEY(super W/5 facilit*) OR TITLE-ABS-KEY(street W/5 facilit*) OR TITLE-ABS-KEY(urban W/5 transport) OR TITLE-ABS-KEY(Street W/5 Transport*) OR TITLE-ABS-KEY(Street W/5 Transit*) OR TITLE-ABS-KEY(road W/5 transport) OR TITLE-ABS-KEY(rail* W/2 Station*) OR TITLE-ABS-KEY(bus W/2 Station*) OR TITLE-ABS-KEY(bus W/2 stop*) OR TITLE-ABS-KEY(park*) OR TITLE-ABS-KEY(underground W/5 rail) OR TITLE-ABS-KEY(underground W/5 station) OR TITLE-ABS-KEY(station W/5 Transit*) OR TITLE-ABS-KEY(system W/5 Transit*) OR TITLE-ABS-KEY(street W/5 walk*) OR TITLE-ABS-KEY(street W/5 pedestrian*) OR TITLE-ABS-KEY(street W/5 freight*) OR TITLE-ABS-KEY(Neighborhood* W/5 design) OR TITLE-ABS-KEY(Neighbourhood* W/5 design) OR TITLE-ABS-KEY(urban W/2 design) OR TITLE-ABS-KEY(building W/5 design) OR TITLE-ABS-KEY(urban W/2 planning) OR TITLE-ABS-KEY("land use") OR TITLE-ABS-KEY(street W/2 design) OR TITLE-ABS-KEY(CRIME W/5 "street light*") OR TITLE-ABS-KEY(intervention W/5 "street light*") OR TITLE-ABS-KEY(intervention W/5 CCTV) OR TITLE-ABS-KEY(crime W/5 CCTV) OR TITLE-ABS-KEY("crime generat*") OR TITLE-ABS-KEY("crime attract*") OR TITLE-ABS-KEY("smart city") OR TITLE-ABS-KEY("smart street") OR TITLE-ABS-KEY(smart W/5 transport) OR TITLE-ABS-KEY(drone) OR TITLE-ABS-KEY(wifi) OR TITLE-ABS-KEY("smart phone") OR TITLE-ABS-KEY("mobile Phone") OR TITLE-ABS-KEY("cell phone") OR TITLE-ABS-KEY(building W/5 sensor*) OR TITLE-ABS-KEY(IoT W/5 device) OR TITLE-ABS-KEY(IoT W/5 urban) OR TITLE-ABS-KEY("big data") OR TITLE-ABS-KEY("cyber") OR TITLE-ABS-KEY("virtual")) AND (TITLE-ABS-KEY (influ* W/5 crime) OR TITLE-ABS-KEY(crime W/5 correlation) OR TITLE-ABS-KEY(crime W/5 spati*) OR TITLE-ABS-KEY(crime W/5 tempo*) OR TITLE-ABS-KEY(crime W/5 spatiotemporal) OR TITLE-ABS-KEY("crime pattern*") OR TITLE-ABS-KEY(Crime W/5 predict*) OR TITLE-ABS-KEY(Crime W/5 forecast*) OR TITLE-ABS-KEY(crime W/2 impact*) OR TITLE-ABS-KEY(crime W/2 affect*) OR TITLE-ABS-KEY(Crime W/2 risk*) OR TITLE-ABS-KEY(Crime W/5 GIS) OR TITLE-ABS-KEY(Distribut* W/5 crime)) AND (TITLE-ABS-KEY (coefficient) OR TITLE-ABS-KEY(Regression*) OR TITLE-ABS-KEY(quantitative* W/2 Analysis) OR TITLE-ABS-KEY(analysis* W/5 regression) OR TITLE-ABS-KEY (econometric W/2 analyses)))

GeoBase:

((built environment) OR (neighborhood*) OR (neighbourhoood*) OR (physical environment) OR (urban place) OR (urban ADJ5 space) OR (urban ADJ5 area*) OR (public ADJ5 realm) OR (micro* ADJ5 place) OR (street ADJ2 urban) OR (street ADJ2 Network) OR (road ADJ2 network) OR (Street Segment) OR (Street configuration) OR (street ADJ5 ecosystem) OR (street ADJ5 traffic) OR (street ADJ5 one-way) OR (Street ADJ5 Two-way) OR (street ADJ5 tree) OR (street ADJ5 green) OR (street ADJ5 furniture) OR (micro ADJ5 facilit*) OR (urban ADJ2 facilit*) OR (super ADJ5 facilit*) OR (street ADJ5 facilit*) OR (urban ADJ5 transport) OR (Street ADJ5 Transport*) OR (Street ADJ5 Transit*) OR (road ADJ5 transport) OR (rail* ADJ2 Station*) OR (bus ADJ2 Station*) OR (bus ADJ2 stop*) OR (park*) OR (underground ADJ5 rail) OR (underground ADJ5 station) OR (station ADJ5 Transit*) OR (system ADJ5 Transit*) OR (street ADJ5 walk*) OR (street ADJ5 pedestrian*) OR (street ADJ5 freight*) OR (Neighborhood* ADJ5 design) OR (Neighbourhood* ADJ5 design) OR (urban ADJ2 design) OR (building ADJ5 design) OR (urban ADJ2 planning) OR (land ADJ1 use*) OR (street ADJ2 design) OR (CRIME ADJ5 street light*) OR (intervention ADJ5 street light*) OR (intervention ADJ5 CCTV) OR (crime ADJ5 CCTV) OR (crime generat*) OR (crime attract*) OR (smart city) OR (smart street) OR (smart ADJ5 transport) OR (drone) OR (wifi) OR (smart phone) OR (mobile Phone) OR (cell phone) OR (building ADJ5 sensor*) OR (IoT ADJ5 device) OR (IoT ADJ5 urban) OR (big data) OR (cyber) OR (virtual)) AND ((influ* ADJ5 crime) OR (crime ADJ5 correlation) OR (crime ADJ5 spati*) OR (crime ADJ5 tempo*) OR (crime ADJ5 spatiotemporal) OR (crime pattern*) OR (Crime ADJ5 predict*) OR (Crime ADJ5 forecast*) OR (crime ADJ2 impact*) OR (crime ADJ2 affect*) OR (Crime ADJ2 risk*) OR (Crime ADJ5 GIS) OR (Distribut* ADJ5 crime))AND ((coefficient) OR (Regression*) OR (quantitative* ADJ2 Analysis) OR (analysis* ADJ5 regression) OR (econometric ADJ2 analyses)))

OR (((built environment) OR (neighborhood*) OR (neighbourhoood*) OR (physical environment) OR (urban place) OR (urban ADJ5 space) OR (urban ADJ5 area*) OR (public ADJ5 realm) OR (micro* ADJ5 place) OR (street ADJ2 urban) OR (street ADJ2 Network) OR (road ADJ2 network) OR (Street Segment) OR (Street configuration) OR (street ADJ5 ecosystem) OR (street ADJ5 traffic) OR (street ADJ5 one-way) OR (Street ADJ5 Two-way) OR (street ADJ5 tree) OR (street ADJ5 green) OR (street ADJ5 furniture) OR (micro ADJ5 facilit*) OR (urban ADJ2 facilit*) OR (super ADJ5 facilit*) OR (street ADJ5 facilit*) OR (urban ADJ5 transport) OR (Street ADJ5 Transport*) OR (Street ADJ5 Transit*) OR (road ADJ5 transport) OR (rail* ADJ2 Station*) OR (bus ADJ2 Station*) OR (bus ADJ2 stop*) OR (park*) OR (underground ADJ5 rail) OR (underground ADJ5 station) OR (station ADJ5 Transit*) OR (system ADJ5 Transit*) OR (street ADJ5 walk*) OR (street ADJ5 pedestrian*) OR (street ADJ5 freight*) OR (Neighborhood* ADJ5 design) OR (Neighbourhood* ADJ5 design) OR (urban ADJ2 design) OR (building ADJ5 design) OR (urban ADJ2 planning) OR (land ADJ1 use*) OR (street ADJ2 design) OR (CRIME ADJ5 street light*) OR (intervention ADJ5 street light*) OR (intervention ADJ5 CCTV) OR (crime ADJ5 CCTV) OR (crime generat*) OR (crime attract*) OR (smart city) OR (smart street) OR (smart ADJ5 transport) OR (drone) OR (wifi) OR (smart phone) OR (mobile Phone) OR (cell phone) OR (building ADJ5 sensor*) OR (IoT ADJ5 device) OR (IoT ADJ5 urban) OR (big data) OR (cyber) OR (virtual)) AND ((influ* ADJ5 crime) OR (crime ADJ5 correlation) OR (crime ADJ5 spati*) OR (crime ADJ5 tempo*) OR (crime ADJ5 spatiotemporal) OR (crime pattern*) OR (Crime ADJ5 predict*) OR (Crime ADJ5 forecast*) OR (crime ADJ2 impact*) OR (crime ADJ2 affect*) OR (Crime ADJ2 risk*) OR (Crime ADJ5 GIS) OR (Distribut* ADJ5 crime))AND ((coefficient) OR (Regression*) OR (quantitative* ADJ2 Analysis) OR (analysis* ADJ5 regression) OR (econometric ADJ2 analyses)))

AND ((abduct*) OR (arson*) OR (assault*) OR (blackmail) OR (bodily harm) OR (burglar*) OR (firearm) OR (weapon) OR (fraud) OR (homicide) OR (kidnapping) OR (manslaughter) OR (murder) OR (prostitut*) OR (public disorder) OR (robber*) OR (shoot*) OR (shoplift*) OR (theft*) OR (vandalism) OR (violen*) OR (terrori*) OR (rape) OR (riot*) OR (anti*social ADJ2 behavio*) OR (knife ADJ2 crim*) OR (money ADJ2 laundering) OR (drug ADJ2 misuse) OR (drug ADJ2 use*) OR (drug ADJ2 possess*) OR (drug ADJ2 deal*) OR (drug ADJ2 traffick*) OR (drug ADJ2 supply) OR (drug ADJ2 market) OR (drug ADJ2 abuse) OR (cyber A DJ5 crime) OR (cyber ADJ5 fraud) OR (cyber ADJ5 security) OR (cyber ADJ5 abuse) OR (Cyber ADJ5 stalk*) OR (Digi* ADJ5 security) OR (digi ADJ5 intervention) OR (DDOS) OR (Ransom)))

Appendix 2

Data extracted from studies included in the Systematic Literature Review:

Study (N=29)	Urban elements	Crime types	Spatial unit	Country	Type of study	Statistical model
Amram et. al. (2024)	number of bus stops (2006), number of businesses (2012), percentage of buildings built in past 10 years, new residential property transactions, community center and educational building within 500m of center of street segment, garden within 150m,	Property and Violence	Street segment	Israel	Cross-sectional study	Zero-inflated negative binomial (ZINB) regression
Beavon et al. (1994)	Street Network & Configuration, Alleyways and drug areas	Property	Street segment	Canada	Matched case-control design	MANOVA
Bernasco & Block (2011)	Street Network & Configuration, Public Transit, Alcohol outlets, Retail land use, barbers' shops and beauty salons, gas stations, laundromats, pawn shops and check cashing services	Violence	Street segment	USA	Cross-sectional study	Negative Binomial Regression Models
Boessena et. al. (2018)	Parks	Property and violence	Census block	USA	Longitudinal study	Negative Binomial Regression Models
Bowers (2014)	Risky facilities – Retail facilities (such as shops and café) and recreational facilities (such as movie theatres and large clubs)	Property	50x50 metre grid cells	UK	Cross-sectional study	Spatial Regression model
Clutter et. al. (2019)	Street Network & Configuration, Public Transit, Parks, Schools, Alcohol outlets, Retail land use, public housing, public libraries, drug treatment centers, hotels, and recreation centers	Violence	Street blocks (segments)	USA	Cross-sectional study	Negative Binomial regression model
Davies & Johnson (2015)	Street Network & Configuration	Property	Street segment	UK	Cross-sectional study	Poisson Hierarchical Linear Model
De Souza & Miller (2012)	Alcohol outlets, Retail land use, alley ways	Violence	50 m to 100-meter area from homicide address	Brazil	Matched case-control design	Ordinary least squares fixed effect Linear Regression model
Deng (2015)	Trees	Violence	Street segment	USA	Cross-sectional study	Multivariate Ordinary Least square Regression Analysis
Favarin (2018)	Street Network & Configuration, Public Transit, Alcohol outlets, Retail land use, Residential land use, mixed land use, public housing, bank branches/ATM, personal care shops, licensed premises, and police stations	Property	Street segment	Italy	Cross-sectional study	Negative Binomial regression model
Groff (2014)	Alcohol outlets	Violence	Street segment (distance of 400 feet)	USA	Cross-sectional study	Zero-inflated Negative Binomial (ZINB)
Groff & Lockwood (2013)	Street Network & Configuration, Public Transit, Schools, Alcohol outlets, drug treatment locations and halfway houses	Violence, property, disorder	Street segment	USA	Cross-sectional study	Negative binomial regression model
Groff & Mccord (2012)	Parks	Violence, property, disorder	50foot buffer around the park	USA	Cross-sectional study	ANOVA

Study (N=29)	Urban elements	Crime types	Spatial unit	Country	Type of study	Statistical model
Haberman & Ratcliffe (2015)	Public Transit, Parks, Schools, Alcohol outlets, Retail land use public housing communities, check-cashing stores, drug treatment centers and pawn shops	Violence	Census block	USA	Cross-sectional study	Binomial Regression analysis
Hsu & Miller (2017)	Public Transit, Parks, Retail land use, Abandoned buildings, vacant land, mailboxes, parking lots, churches	Drug	Street segments and interactions	USA	Matched case-control design	Conditional Logistic Regression Model
Johnson & Bowers (2009)	Street Network & Configuration	Property	Street segment	UK	Cross-sectional study	Poisson Hierarchical Linear Model
Kim & Hipp (2019)	Street Network & Configuration, Retail land use	Property and Violence	Street segment	USA	Cross-sectional study	Negative Binomial regression model
Kim & Hipp (2022)	Physical boundaries (as land use difference – residential, retail, office, industry and other between the two sides of the street)	Property and Violence	Street segments within a 20-m (65 feet) buffer	USA	Cross-sectional study	Negative Binomial Regression model
Kim & Wo (2023)	Physical topological features of street segments (effects of elevation, slope, and street connectivity i.e. betweenness within 1/4th mile on crime)	Property and Violence	Street segment	USA	Cross-sectional study	Negative Binomial Regression
Kim & Wo (2022)	Retail (stores, shopping mall, restaurant), hotel, school	Property and Violence	Census Block	USA	Cross-sectional study	Logistic Regression
Lee & Contreras (2021)	Walkability	Property and Violence	Census Block	USA	Cross-sectional study	Negative Binomial Regression
Liggett et al. (2003)	Public Transit, Alcohol outlets	Violence, disorder, property and drug	46m (150ft) radius of intersections where bus stops were located	USA,	Cross-sectional study	Regression analysis
Newton (2014)	Public Transit	Property	400m buffer zone around stations	UK	Cross-sectional study	Negative Binomial Poisson regression model
Ratcliffe (2012)	Public Transit, Schools, Alcohol outlets, fire stations	Violence	85 feet from centroid of the bars	USA	Cross-sectional study	Change point Poisson regression
Soohyun & Yongjei (2016)	Public Transit, Schools, Retail land use	Property, Violence, Disorder and all crimes	500-ft ² grid cells	USA	Cross-sectional study	Multivariate Linear Regression Analysis
Summers & Johnson (2016)	Street network & configuration	Outdoor serious violence	Street segment	UK - England	Cross-sectional study	Zero-inflated Negative Binomial (ZINB)
Vilalta & Fondevila (2019)	Street network & configuration, Alcohol outlets, Retail land use	Violence	Census block	Mexico	Cross-sectional study	Geographically weighted Poisson regression model
Wo & Park (2020)	Schools	Property and Violence	Census Block	USA	Cross-sectional study	Negative Binomial Regression
Xie et al. (2022)	road density in the areas surrounding the street segments, walkability, the greening rate and the number of - streetlamps, sidewalks, enclosure effects, fences, buildings, grass, walls and trees – in streetscape	Property	Street segment	China	Cross-sectional study	Machine learning model

Appendix 3

1. Combined effect sizes that determine influence of Street Configuration on crime (Chapter 3, Section 3.3.1.2)

Authors and Year of Study	Effect size (Coeff)	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR EXP (coeff)	Std Error of IRR	EXP (LCI)	EXP (UCI)	z	Significance
Data for which meta-analysis was conducted											
Property crimes, predictor variable -Main roads											
Johnson & Bowers, 2010 (Property crimes-Main Road)	0.199	0.038	0.074	0.125	0.273	1.220		1.133	1.314	5.25	P<0.01
Groff & Lockwood, 2014 (Property crimes-Main Road)	0.610	0.016	0.032	0.578	0.642	1.840	0.03	1.782	1.900		P<0.001
Combined (Property crimes-Main Road (2 studies))	0.407	0.145	0.284	0.123	0.692	1.502	1.131	1.502	1.131	p<0.01	
Davies & Johnson, 2015 (Property crimes-Betweenness)	0.811	0.050	0.098	0.713	0.909	2.250		2.040	2.481	16.24	P<.05
Kim & Wo, 2023 (Property crimes-Burglary-Betweenness)	-0.008	0.002	0.003	-0.011	-0.005	0.992		0.989	0.995	4.921	Not significant
Combined (Property crimes-Betweenness (2 studies, lowest value))	0.398	0.289	0.567	-0.169	0.966	1.489		0.845	2.627	Not significant	
Kim & Wo, 2023 (Property crimes-MVT-Betweenness)	0.027	0.006	0.011	0.016	0.038	1.027		1.016	1.039	4.692	p < .01
Combined (Property crimes-Betweenness (2 studies, highest value))	0.554	0.209	0.409	0.145	0.964	1.740		1.156	2.622	p<0.05	

Authors and Year of Study	Effect size (Coeff)	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR EXP (coeff)	Std Error of IRR	EXP (LCI)	EXP (UCI)	z	Significance
Violent crimes, predictor variable -Main Roads											
Groff & Lockwood, 2014 (Violent crimes- Main Road)	0.565	0.017	0.033	0.532	0.599	1.760	0.030	1.702	1.820		P<0.001
Bernasco & Block, 2011 (Violent crimes- Main Road)	0.448	0.022	0.044	0.404	0.492	1.565		1.498	1.635		P<0.001
Vilalta & Fondevila, 2019 (Violent crimes- Main Road)	1.107	0.070	0.137	0.970	1.243	3.024	0.211	2.637	3.467		P<0.01
Combined (Violent crimes- Main Road (3 studies))	0.699	0.163	0.319	0.380	1.018	2.012		1.462	2.768		p<0.001
Violent crimes, predictor variable - Betweenness											
Clutter et al., 2019 (Violent crimes-Robbery- Betweenness)	0.266	0.032	0.062	0.204	0.328	1.305		1.226	1.388		P<0.001
Summers & Johnson, 2017 (Violent crimes- Betweenness)	0.275	0.067	0.131	0.143	0.406	1.316		1.154	1.501	4.094	P<0.01
Kim & Wo, 2023 (Violent crimes- Aggravated Assault - Betweenness, lowest value)	0.024	0.005	0.010	0.014	0.034	1.024		1.014	1.034	4.848	Not significant
Combined (Violent crimes- Betweenness (3 studies, lowest value))	0.179	0.070	0.138	0.041	0.317	1.196		1.042	1.373		p<0.01
Kim & Wo, 2023 (Violent crimes- Robbery - Betweenness, highest value)	0.088	0.020	0.039	0.049	0.127	1.092		1.050	1.136	4.389	p < .01
Combined for 6 studies - lowest value (8data points)- Violent crimes	0.200	0.052	0.102	0.098	0.303	1.221		1.103	1.354		p<0.001

Authors and Year of Study	Effect size (Coeff)	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR EXP (coeff)	Std Error of IRR	EXP (LCI)	EXP (UCI)	z	Significance
Data for which meta-analysis could not be conducted (Depicted on Forest plot only)											
Kim & Wo, 2023 (Property Crimes-Burglary-Elevation(ft))	-0.022	0.005	0.009	-0.031	-0.013	0.978		0.970	0.987	4.8746	Not significant
Kim & Wo, 2023 (Property crimes-Burglary-Slope (%))	-0.034	0.007	0.014	-0.048	-0.020	0.967		0.953	0.980	4.7598	p < .05
Kim & Wo, 2023 (Property crimes-Burglary-SD of elevation)	-0.036	0.008	0.015	-0.051	-0.021	0.965		0.950	0.979	4.7475	p < .05
Kim & Wo, 2023 (Property crimes-MVT-Elevation(ft))	-0.061	0.013	0.026	-0.087	-0.035	0.941		0.917	0.966	4.597	p < .01
Kim & Wo, 2023 (Property crimes-MVT-Slope(%))	0.010	0.002	0.004	0.006	0.014	1.010		1.006	1.014	4.9202	Not significant
Kim & Wo, 2023 (Property crimes-MVT-SD of elevation)	-0.006	0.001	0.002	-0.008	-0.004	0.994		0.992	0.996	4.9566	Not significant
Kim & Wo, 2023 (Property crimes-Larceny-Elevation(ft))	-0.171	0.045	0.088	-0.259	-0.083	0.843		0.772	0.920	3.8173	p < .01
Kim & Wo, 2023 (Property crimes-Larceny-Slope (%))	-0.026	0.005	0.011	-0.037	-0.015	0.974		0.964	0.985	4.7785	p < .05
Kim & Wo, 2023 (Property crimes-Larceny-SD of elevation)	-0.070	0.016	0.031	-0.101	-0.039	0.932		0.904	0.962	4.4518	p < .01

Authors and Year of Study	Effect size (Coeff)	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR EXP (coeff)	Std Error of IRR	EXP (LCI)	EXP (UCI)	z	Significance
Kim & Wo, 2023 (Violent Crimes-Aggravated Assault--Elevation(ft))	-0.032	0.007	0.013	-0.045	-0.019	0.969		0.956	0.981	4.8866	Not significant
Kim & Wo, 2023 (Violent crimes-Aggravated Assault-Slope (%))	-0.025	0.005	0.010	-0.035	-0.015	0.975		0.966	0.985	4.8858	Not significant
Kim & Wo, 2023 (Violent Crimes-Aggravated Assault-SD of elevation)	-0.037	0.008	0.015	-0.052	-0.022	0.964		0.949	0.978	4.8425	Not significant
Kim & Wo, 2023 (Violent crimes-Robbery-Elevation(ft))	0.020	0.004	0.008	0.012	0.028	1.020		1.012	1.028	4.9205	Not significant
Kim & Wo, 2023 (Violent crimes-Robbery-Slope (%))	-0.042	0.009	0.017	-0.059	-0.025	0.959		0.942	0.976	4.7725	p < .05
Kim & Wo, 2023 (Violent crimes Robbery-SD of elevation)	-0.080	0.017	0.034	-0.114	-0.046	0.923		0.892	0.955	4.5827	p < .01
Groff & Lockwood, 2014 (Disorder crimes- Main Road)	0.737	0.033	0.066	0.672	0.803	2.090	0.07	1.957	2.232		P<0.001
Data Legend Provided Calculated											

2. Combined effect sizes that determine influence of Public Transit on crime (Chapter 3, Section 3.3.2.1)

Authors and Year of Study	Effect size (Coeff)	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR EXP (coeff)	Std Error of IRR	EXP (LCI)	EXP (UCI)	z	Significance
Data for which meta-analysis was conducted											
Property crimes, Predictor variable –Public Transit stops											
Amram et. al. (2024) - Property crimes - Bus stops	0.0710	0.0320	0.0627	0.0083	0.1337	1.0740		1.0083	1.1431		P<0.1
Groff & Lockwood (2014) - Property crimes - Subway stops	0.6575	0.0777	0.1523	0.5052	0.8099	1.9300	0.15	1.6573	2.2476		P<0.001
Favarin (2018) - Property crime (Burglary)-Bus and Tram stops (Assumed slightly insignificant)	-0.0190	0.0148	0.0291	-0.0481	0.0101	0.9812		0.9531	1.0101	1.28	P=0.1 (Not significant (p>0.05))
Combined (Property crimes - Transit (3 studies)) - Lowest value	0.2360	0.1730	0.3390	-0.1030	0.5750	1.2662		0.9021	1.7771		p>0.05, Not significant
Favarin (2018) - Property crime (Burglary)-Bus and Tram stops (Assumed highly insignificant)	-0.0190	0.7579	1.4854	-1.5044	1.4664	0.9812		0.2221	4.3338	0.02	P=0.51 (Not significant p>0.05)
Combined (Property crimes - Transit (2 studies)) - Highest value	0.3330	0.1959	0.3840	-0.0510	0.7180	1.3951		0.9503	2.0503		p<0.05
Violent crimes, Predictor variable –Public Transit stops											
Amram et. al. (2024) - Violent crimes - Bus stops	0.0510	0.0330	0.0647	-0.0137	0.1157	1.0520		0.9864	1.1226		p<0.1
Groff & Lockwood (2014) - Violent crimes - Subway stops	1.0080	0.0657	0.1288	0.8792	1.1367	2.7400	.180	2.4090	3.1165		p<0.001
Favarin (2018) - Violent crimes - Bus and Tram stops	0.1570	0.0664	0.1301	0.0269	0.2871	1.1700		1.0273	1.3325	2.36	P=.009 (p<0.01)
Bernasco & Block (2011) - Violent crimes - EL station	1.4390	0.0976	0.1913	1.2477	1.6303	4.2165		3.4823	5.1054		Significant
Clutter et al. (2019) –Violent crimes - Bus stops (presence of bus stop)	0.6804	0.1124	0.2203	0.4601	0.9007	1.9747		1.5842	2.4613		P<0.001
Haberman & Ratcliffe (2015) - Violent crimes - Subway stop (Robbery) – Morning data	0.5040	0.3210	0.6292	-0.1252	1.1332	1.6560		0.8824	3.1055		Not significant (p>0.05)
Combined (Violent crimes - Transit (5 studies)) - Lowest Value	0.6420	0.328	0.6420	0.2410	1.0440	1.9003		1.2725	2.8406		p<0.001

Authors and Year of Study	Effect size (Coeff)	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR EXP (coeff)	Std Error of IRR	EXP (LCI)	EXP (UCI)	z	Significance
Haberman & Ratcliffe (2015) - Violent crimes - Subway stop (Robbery)- Evening data	0.6890	0.1600	0.3136	0.3754	1.0026	1.992		1.4556	2.7254		P<0.001
Combined (Violent crimes - Transit (5 studies)) - Highest value	0.8180	0.2190	0.3136	0.3754	1.0026	1.9920		1.4556	2.7254		p<0.001
Data for which meta-analysis could not be conducted (Depicted on Forest plot only)											
Groff & Lockwood (2014) - Disorder crimes - Subway stops	0.9933	0.1111	0.2178	0.7755	1.2110	2.7000	0.300	2.1716	3.3569		P<0.001
Data Legend Provided Calculated											

3. Combined effect sizes that determine influence of Parks on crime (Chapter 3, Section 3.3.3.1)

Authors and Year of Study	Effect size (Coeff)	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR EXP (coeff)	Std Error of IRR	EXP (LCI)	EXP (UCI)	z	t-value	Significance
Data for which meta-analysis was conducted												
Robbery (Violent) crimes, Predictor variable – Block has a park												
Boessen et. al (2018), Violent crimes (Robbery) - Block has a Park	0.073	0.014913	0.02923	0.0438	0.1022	1.0757		1.0447	1.1076	4.895	1.050	Not significant (p>0.05)
Clutter et al. (2019), Violent crimes (Robbery) - Presence of Parks	-0.0501	0.2279	0.446684	0.4968	0.3966	0.9511		0.6085	1.4867			Not significant (p>0.05)
Haberman & Ratcliffe (2015), Violent crimes (Robbery) Parks - morning	0.618	0.301	0.58996	0.0280	1.2080	1.8552		1.0284	3.3467			p < .05
Combined (lowest in morning), Robbery - Presence of Parks (3 studies)	0.074	0.014796	0.029	0.0450	0.1030	1.0768		1.0460	1.1085			p<0.001
Haberman & Ratcliffe (2015), Violent crimes (Robbery) Parks - day time	0.572	0.181	0.35476	0.2172	0.9268	1.7718		1.2426	2.5263			p < .05
Combined (highest in daytime) - Robbery, Presence of Parks (3 studies)	0.176	0.123469	0.242	0.0660	0.4180	1.1924		0.9361	1.5189			p>0.05 Not Significant
Data for which meta-analysis could not be conducted (Depicted on Forest plot only)												
Boessen et. al (2018), Violent crimes (Robbery) - Size of park	-0.014	0.002854	0.005593	0.0196	0.0084	0.9861		0.9806	0.9916	4.906	0.940	Not significant (p>0.05)

Authors and Year of Study	Effect size (Coeff)	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR EXP (coeff)	Std Error of IRR	EXP (LCI)	EXP (UCI)	z	t-value	Significance
Boessen et. al (2018), Violent crimes (Robbery)- park is within 400 ft of block	-0.063	0.013328	0.026122	0.0891	0.0369	0.9389		0.9147	0.9638	4.727	2.730	p<0.01
Boessen et. al (2018), Violent crimes (Aggravated Assault)- Block has a Park	0.145	0.030271	0.059332	0.0857	0.2043	1.1560		1.0894	1.2267	4.790	2.100	p<0.05
Boessen et. al (2018), Violent crimes (Aggravated Assault)- Size of park in a block	-0.001	0.0002	0.000393	0.0014	0.0006	0.9990		0.9986	0.9994	4.988	0.120	Not significant (p>0.05)
Boessen et. al (2018), Violent crimes (Aggravated Assault)- park is within 400 ft of block	-0.019	0.003885	0.007614	0.0266	0.0114	0.9812		0.9737	0.9887	4.891	1.090	Not significant (p>0.05)
Boessen et. al (2018), Violent crimes (Homicide)- Block has a Park	0.273	0.05637	0.110485	0.1625	0.3835	1.3139		1.1765	1.4674	4.843	1.570	Not significant (p>0.05)
Boessen et. al (2018), Violent crimes (Homicide)-Size of park	-0.019	0.003829	0.007505	0.0265	0.0115	0.9812		0.9738	0.9886	4.962	0.380	Not significant (p>0.05)
Boessen et. al (2018), Violent crimes (Homicide)-park is within 400 ft of block	-0.118	0.024568	0.048153	0.1662	0.0698	0.8887		0.8469	0.9325	4.803	1.970	p<0.05
Boessen et. al (2018), Property crime (Burglary)- Block has a park	-0.9	0.187149	0.366812	1.2668	0.5332	0.4066		0.2817	0.5867	4.809	1.91	Not significant (p>0.05)

Boessen et. al (2018), Property crime (Burglary)-Size of park	0.012	0.002475	0.00485	0.0071	0.0169	1.0121		1.0072	1.0170	4.849	1.51	Not significant (p>0.05)
Boessen et. al (2018), Property crime (Burglary)-Block is within 400 ft of park	-0.013	0.002649	0.005192	0.0182	0.0078	0.9871		0.9820	0.9922	4.908	0.92	Not significant (p>0.05)
Boessen et. al (2018), Property crime (Motor theft)-Block has a park	0.013	0.002613	0.005121	0.0079	0.0181	1.0131		1.0079	1.0183	4.976	0.24	Not significant (p>0.05)
Boessen et. al (2018), Property crime (Motor theft)-Size of park	-0.011	0.002262	0.004434	0.0154	0.0066	0.9891		0.9847	0.9935	4.862	1.38	Not significant (p>0.05)
Boessen et. al (2018), Property crime (Motor theft)-Block is within 400 ft of park	-0.075	0.016597	0.032529	0.1075	0.0425	0.9277		0.8981	0.9584	4.519	4.81	p<0.01
Boessen et. al (2018), Property crime (Larceny)-Block has a park	-0.069	0.014145	0.027724	0.0967	0.0413	0.9333		0.9078	0.9596	4.878	1.22	Not significant (p>0.05)
Boessen et. al (2018), Property crime (Larceny)-Size of park	-0.003	0.000605	0.001185	0.0042	0.0018	0.9970		0.9958	0.9982	4.962	0.38	Not significant (p>0.05)
Boessen et. al (2018), Property crime (Larceny)-Block is within 400 ft of park	-0.056	0.012061	0.02364	0.0796	0.0324	0.9455		0.9234	0.9682	4.643	3.57	p<0.01
Data Legend Provided Calculated												

4. Combined effect sizes that determine influence of Schools on crime (Chapter 3, Section 3.3.4.1)

Authors and Year of Study	Unstd. Coefficient	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR	Std Error of IRR	EXP (LCI)	EXP (UCI)	z	Significance
Data for which meta-analysis could not be conducted (Depicted on Forest plot only)											
Property crimes, Predictor variable - schools											
Property crimes - All schools, Wo & Park (2020)	0.427	0.043	0.084	0.343	0.511	1.533		1.088	1.409		p>0.01
Property crimes - Non elementary Schools, Groff & Lockwood (2014)	-0.010	0.061	0.119	-0.129	0.109	0.990	0.060	0.879	1.115		Not significant
Property crimes - Schools (Burglary), (Assumed slightly insignificant), Favarin (2018)	0.028	0.022	0.043	-0.015	0.071	1.028		0.985	1.073	1.282	Not significant, Assume p=0.1
Combined (Property crimes-Schools (3 studies)) - Lowest value	0.149	0.114	0.223	-0.074	0.373	1.161		0.929	1.452	P>0.5 Not Significant	
Property crimes - Schools (Burglary) , (Assumed highly insignificant) , Favarin (2018)	0.028	1.120	2.195	-2.167	2.223	1.028		0.114	9.237	0.025	Not significant, Assume p=0.51
Combined (Property crimes-Schools (3 studies)) - Highest value	0.2100	0.152	0.298	-0.0880	0.5070	1.234		0.916	1.660	P>0.5 Not Significant	
Violent crimes, Predictor variable - schools											
Violent crimes - All schools, Wo & Park (2020)	0.300	0.006	0.012	0.288	0.312	1.350		1.012	1.334		P<0.01
Violent crimes - Non elementary Schools, Groff & Lockwood (2014)	-0.010	0.071	0.139	-0.149	0.129	0.990	0.070	0.862	1.137		Not significant
Violent crimes - High schools (Robberies), Clutter et al., 2019	-0.507	0.354	0.693	-1.201	0.186	0.602		0.301	1.205		Not significant
Violent crimes - High schools (Robbery) - late night (Lowest value), Haberman & Ratcliffe (2015)	0.466	0.153	0.300	0.166	0.766	1.593		1.181	2.151		p<0.01
Combined Violent crimes-Schools (4 studies)) - Lowest value	0.17	0.114	0.224	-0.0540	0.3950	1.185		0.947	1.484	P>0.5 Not Significant	
Violent crimes - High schools (Robbery) - evening (Highest value), Haberman & Ratcliffe (2015)	0.756	0.195	0.382	0.374	1.138	2.129		1.453	3.121		p<0.001
Combined Violent crimes-Schools (4 studies)) - Highest value	0.196	0.179	0.350	-0.1540	0.5470	1.217		0.857	1.728	P>0.5 Not Significant	
Data for which meta-analysis could not be conducted (Depicted on Forest plot only)											
Violent crimes - Higher Education (Robberies), Clutter et al., 2019	-1.252	0.512	1.004	-2.256	-0.248	0.286		0.105	0.780		p<0.05
Disorder crimes - Non elementary Schools, Groff & Lockwood (2014)	1.391	0.061	0.119	1.272	1.510	4.020	0.350	3.570	4.527		p<0.001
Data Legend											
		Provided		Calculated							

5. Combined effect sizes that determine influence of Alcohol outlets on crime (Chapter 3, Section 3.3.5.1)

Authors and Year of Study	Effect size (Coeff)	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR EXP (coeff)	Std Error of IRR	EXP (LCI)	EXP (UCI)	z	Significance
Data for which meta-analysis was conducted											
Property crimes, predictor variable -presence of alcohol outlets											
Groff & Lockwood (2014), Property crimes - Bars	0.131	0.009	0.017	0.114	0.148	1.140	0.010	1.121	1.160		p<0.001
Favarin (2018), Property crimes (Burglary) - Licenced Premises	0.099	0.042	0.082	0.017	0.181	1.104		1.198	3.016	2.366	p<0.01
Combined for 2 studies, Property crimes	0.130	0.009	0.017	0.113	0.146	1.139		1.120	1.157		p<0.001
Violent crimes, predictor variable -presence of alcohol outlets											
Groff & Lockwood (2014), Violent crimes - Bars	0.086	0.009	0.018	0.068	0.104	1.090	0.010	1.071	1.110		p<0.001
Favarin (2018), Violent crimes - Licenced Premises	0.055	0.023	0.046	0.010	0.101	1.057		1.010	1.107	2.366	p<0.01
Clutter et al., 2019, Violent crimes - Robberies - drinking places	0.251	0.215	0.421	-0.170	0.673	1.286		0.844	1.960		Not significant
Vilalta & Fondevila (2019), Violent crimes- Alcohol outlets	0.234	0.038	0.074	0.160	0.309	1.264	0.048	1.173	1.362		P<0.01
Bernasco & Block (2011), Violent crimes - Number of bars and clubs with <less than 10 employees (lowest value)	0.169	0.037	0.073	0.096	0.242	1.184		1.101	1.274		p<0.001

Authors and Year of Study	Effect size (Coeff)	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR EXP (coeff)	Std Error of IRR	EXP (LCI)	EXP (UCI)	z	Significance
Haberman & Ratcliffe (2015), Violent crimes - Alcohol stores (Robbery) - morning (lowest value)	-0.609	0.449	0.880	-1.489	0.271	0.544		0.226	1.311		Not significant
Combined for 6 studies - lowest value, Violent crimes	0.095	0.037	0.072	0.023	0.167	1.100		1.023	1.182	p<0.01	
Bernasco & Block (2011), Violent crimes - Robberies - Number of Liquor stores (highest value)	0.514	0.060	0.117	0.397	0.630	1.671		1.487	1.878		p<0.001
Haberman & Ratcliffe (2015), Violent crimes - Bars (Robbery) - day time (highest value)	0.144	0.088	0.172	-0.028	0.316	1.155		0.972	1.372		Not significant
Combined for 6 studies - highest value, Violent crimes	0.205	0.068	0.134	0.071	0.339	1.228		1.074	1.404	p<0.01	
Data for which meta-analysis could not be conducted (Depicted on Forest plot only)											
Disorder crimes, predictor variable -presence of alcohol outlets											
Groff & Lockwood (2014), Disorder crimes - Bars	0.399	0.009	0.017	0.382	0.416	1.465		1.516	0.025		p<0.001
Data Legend Provided Calculated											

6. Combined effect sizes that determine influence of Retail land use on crime (Chapter 3, Section 3.3.6.1)

Authors and Year of Study	Unstd. Coefficient	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR	Std Error of IRR	EXP (LCI)	EXP (UCI)	z value	Significance
Data for which meta-analysis was conducted											
Property crimes – Retail land use											
Property crimes- (External theft), All Retail land parcels, Bowers (2014)	0.770	0.159	0.312	0.458	1.082	2.160		1.581	2.950	4.838	Not significant
Favarin (2018), Property crimes (Burglary) - Combined Retail shops including licenced premises and personal care	0.026	0.007	0.014	0.012	0.041	1.026		1.012	1.042		
Combined (Property crimes-Retail (2 studies))	0.364	0.261	0.511	-0.147	0.875	1.439		0.863	2.399		Insignificant
Violent crimes – Retail land use											
Vilalta & Fondevila (2019), Violent crimes - (including No Alcohol outlets and alcohol outlets)	0.112	0.081	0.159	-0.047	0.272	1.119		0.954	1.313		p<0.01
Bernasco & Block (2011), Violent crimes - Robberies - combined Retail	0.349	0.038	0.075	0.274	0.424	1.418		1.315	1.528		
Clutter et al., (2019), Violent crimes - (Robberies), Combined Retail	0.194	0.117	0.230	-0.036	0.424	1.214		0.965	1.528		
Favarin (2018), Violent crimes (Robbery) - Retail shops including licenced premises and personal care	0.013	0.020	0.039	-0.026	0.053	1.013		0.974	1.054	2.366	p<0.01
Haberman & Ratcliffe (2015), Violent crimes - Combined Retail - evening time (lowest value)	0.148	0.026	0.051	0.097	0.199	1.160		1.102	1.220		
Combined Violent crimes-Retail (5 studies) - Lowest value	0.160	0.057	0.111	0.049	0.271	1.174		1.050	1.311		p<0.01
Haberman & Ratcliffe (2015), Violent crimes - Combined Retail - afternoon time (highest value)	0.184	0.027	0.053	0.131	0.237	1.202		1.140	1.267		
Combined Violent crimes-Retail (5 studies) - Highest value	0.169	0.057	0.112	0.057	0.280	1.184		1.059	1.323		p<0.01
Data Legend											
				Provided		Calculated					

The effect sizes of individual retail land uses were combined within the studies prior to conducting data synthesis across studies.

Author and Year of study	Coefficient	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR
Favarin (2018), Property crimes (Burglary) - Retail shops excluding licenced premises and personal care	0.030	0.013	0.025	0.005	0.054	1.030
Favarin (2018), Property crimes (Burglary) - Personal care shops	0.025	0.011	0.021	0.004	0.046	1.025
Favarin (2018), Property crimes (Burglary) -Licenced premises	0.099	0.042	0.082	0.017	0.181	1.104
Favarin (2018), Property crimes (Burglary) - Combined Retail shops including licenced premises and personal care	0.026	0.007	0.014	0.012	0.041	1.026
Author and Year of study	Coefficient	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR
Kim & Hipp (2019), Property crimes (Burglary) - Retail businesses	- 0.170	0.022	0.044	-0.214	-0.126	0.844
Kim & Hipp (2019), Property crimes - Restaurants	- 0.091	0.015	0.028	-0.119	-0.063	0.913
Kim & Hipp (2019), Property crimes - Stores	- 0.191	0.026	0.052	-1.243	-0.139	0.826
Kim & Hipp (2019), Property crimes (Burglary) - Combined Retail shops including Retail businesses, restaurants and stores	-0.147	0.026	0.050	-0.197	-0.096	0.863

Author and Year of study	Coefficient	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR
Bernasco & Block (2011), Violent crimes - Nr. of general merchandise stores	0.499	0.094	0.183	0.315	0.682	1.647
Bernasco & Block (2011), Violent crimes - Nr of groceries	0.295	0.031	0.061	0.234	0.357	1.344
Bernasco & Block (2011), Violent crimes - Nr. of gas stations	0.410	0.036	0.071	0.339	0.481	1.507
Bernasco & Block (2011), Violent crimes - Nr. of fastfood restaurants < 10 employees	0.252	0.023	0.045	0.207	0.297	1.286
Bernasco & Block (2011), Violent crimes - Barbers and beauty salons < 10 employees	0.244	0.020	0.040	0.204	0.284	1.277
Bernasco & Block (2011), Violent crimes - Nr. of laundromats	0.456	0.070	0.137	0.319	0.592	1.577
Bernasco & Block (2011), Violent crimes - Nr. pawn cheques and cheque-cash services	0.425	0.040	0.079	0.346	0.503	1.529
Bernasco & Block (2011), Violent crimes - Number of bars and clubs with <less than 10 employees	0.169	0.037	0.073	0.096	0.242	1.184
Bernasco & Block (2011), Violent crimes - Robberies - Number of Liquor stores	0.514	0.060	0.117	0.397	0.630	1.671
Bernasco & Block (2011), Combined Violent crimes - Robberies - Retail	0.349	0.038	0.075	0.274	0.424	1.418

Author and Year of study	Coefficient	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR
Clutter et al., (2019), Violent crimes (Robberies), Retail stores	0.022	0.065	0.128	-0.106	0.150	1.022
Clutter et al., (2019), Violent crimes (Robberies), Everyday stores	0.699	0.120	0.234	0.464	0.933	2.011
Clutter et al., (2019), Violent crimes (Robberies), Grocery stores	0.264	0.467	0.916	-0.651	1.180	1.302
Clutter et al., (2019), Violent crimes (Robberies), Eating places/ Restaurants	-0.017	0.083	0.162	-0.178	0.145	0.983
Clutter et al., (2019), Violent crimes (Robberies), Check cashing and pawn	0.508	0.494	0.967	-0.459	1.475	1.662
Clutter et al., (2019), Violent crimes (Robberies), Salons/barbers	0.113	0.278	0.544	-0.431	0.657	1.120
Clutter et al., (2019), Violent crimes (Robberies), Laundry	-1.131	0.729	1.429	-2.560	0.297	0.323
Clutter et al., (2019), Violent crimes (Robberies), Body art parlors	0.204	0.633	1.240	-1.036	1.443	1.226
Clutter et al., (2019), Violent crimes - (Robberies), Drinking places	0.251	0.215	0.421	-0.170	0.673	1.286
Clutter et al., (2019), Violent crimes - (Robberies), Combined Retail	0.194	0.117	0.230	-0.036	0.424	1.214
Author and Year of study	Coefficient	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR
Haberman & Ratcliffe (2015), Violent crimes - Corner stores - (Morning)	0.367	0.090	0.176	0.191	0.543	1.443
Haberman & Ratcliffe (2015), Violent crimes - Fast food restaurants - (Morning)	0.115	0.058	0.114	0.001	0.229	1.122
Haberman & Ratcliffe (2015), Violent crimes - Check cashing stores - (Morning)	0.074	0.209	0.410	-0.336	0.484	1.077
Haberman & Ratcliffe (2015), Violent crimes - pawn shops - (Morning)	0.739	0.939	1.840	-1.101	2.579	2.095
Haberman & Ratcliffe (2015), Violent crimes - bars - (Morning)	0.070	0.155	0.304	-0.234	0.374	1.072
Haberman & Ratcliffe (2015), Violent crimes - Alcohol stores - (Morning)	-0.609	0.449	0.880	-1.489	0.271	0.544
Haberman & Ratcliffe (2015), Violent crimes - Combined Retail - (Morning)	0.167	0.068	0.134	0.033	0.302	1.182

Author and Year of study	Coefficient	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR
Haberman & Ratcliffe (2015), Violent crimes - Corner stores - (Afternoon)	0.254	0.058	0.114	0.140	0.368	1.290
Haberman & Ratcliffe (2015), Violent crimes - Fast food restaurants - (Afternoon)	0.155	0.035	0.069	0.086	0.224	1.167
Haberman & Ratcliffe (2015), Violent crimes - Check cashing stores - (Afternoon)	0.271	0.114	0.223	0.048	0.494	1.311
Haberman & Ratcliffe (2015), Violent crimes - pawn shops - (Afternoon)	0.850	0.322	0.631	0.219	1.481	2.339
Haberman & Ratcliffe (2015), Violent crimes - bars - (Afternoon)	0.144	0.088	0.172	-0.028	0.316	1.155
Haberman & Ratcliffe (2015), Violent crimes - alcohol stores - (Afternoon)	0.071	0.145	0.284	-0.213	0.355	1.073
Haberman & Ratcliffe (2015), Violent crimes - Combined Retail - (Afternoon)	0.184	0.027	0.053	0.131	0.237	1.202
Author and Year of study	Coefficient	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR
Haberman & Ratcliffe (2015), Violent crimes - Corner stores - (Evening)	0.224	0.056	0.110	0.114	0.334	1.251
Haberman & Ratcliffe (2015), Violent crimes - Fast food restaurants - (Evening)	0.141	0.034	0.067	0.074	0.208	1.151
Haberman & Ratcliffe (2015), Violent crimes - Check cashing stores - (Evening)	0.242	0.106	0.208	0.034	0.450	1.274
Haberman & Ratcliffe (2015), Violent crimes - pawn shops - (Evening)	0.432	0.241	0.472	-0.040	0.904	1.537
Haberman & Ratcliffe (2015), Violent crimes - Bars - (Evening)	0.016	0.083	0.163	-0.147	0.179	1.016
Haberman & Ratcliffe (2015), Violent crimes - Alcohol stores - (Evening)	-0.076	0.137	0.269	-0.345	0.193	0.927
Haberman & Ratcliffe (2015), Violent crimes - Combined Retail - (Evening)	0.148	0.026	0.051	0.097	0.199	1.160

Author and Year of study	Coefficient	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR
Haberman & Ratcliffe (2015), Violent crimes - Corner stores - (Late night)	0.231	0.042	0.082	0.149	0.313	1.260
Haberman & Ratcliffe (2015), Violent crimes - Fast food restaurants - (Late night)	0.138	0.031	0.061	0.077	0.199	1.148
Haberman & Ratcliffe (2015), Violent crimes - Check cashing stores - (Late night)	0.296	0.098	0.192	0.104	0.488	1.344
Haberman & Ratcliffe (2015), Violent crimes - pawn shops - (Late night)	0.219	0.244	0.478	-0.259	0.697	1.244
Haberman & Ratcliffe (2015), Violent crimes - Bars - (Late night)	0.113	0.060	0.118	-0.005	0.231	1.120
Haberman & Ratcliffe (2015), Violent crimes - Alcohol stores - (Late night)	-0.045	0.116	0.227	-0.272	0.182	0.956
Haberman & Ratcliffe (2015), Violent crimes - Combined Retail - (Late night)	0.163	0.028	0.054	0.109	0.217	1.177

Author and Year of study	Coefficient	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR
Favarin (2018), Violent crimes (Robbery) - Retail shops excluding licenced premises and personal care	0.058	0.025	0.048	0.010	0.107	1.060
Favarin (2018), Violent crimes (Robbery) - Personal care shops	0.023	0.010	0.019	0.004	0.042	1.023
Favarin (2018), Property crimes (Robbery) - Licenced premises	0.055	0.023	0.046	0.010	0.101	1.057
Favarin (2018), Violent crimes (Robbery) - Combined Retail shops including licenced premises and personal care	0.013	0.020	0.039	-0.026	0.053	1.013
Authors and Year of Study	Coefficient	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR
Vilalta & Fondevila (2019), Violent crimes - No Alcohol outlets (excluding alcohol outlets)	0.003	0.001	0.002	0.001	0.005	1.003
Vilalta & Fondevila (2019), Violent crimes - Alcohol outlets	0.234	0.038	0.074	0.160	0.309	1.26
Vilalta & Fondevila (2019), Violent crimes - Combined (including No Alcohol outlets and alcohol outlets)	0.112	0.081	0.159	-0.047	0.272	1.119

7. Combined effect sizes that determine influence of Drug Treatment Centres on crime (Chapter 3, Section 3.3.7)

Authors and Year of Study	Effect size (Coeff)	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR EXP (Coeff)	Std Error of IRR	EXP (LCI)	EXP (UCI)	z	Significance
Data for which meta-analysis was conducted											
Violent crimes (Robberies)-Drug Treatment Centres , Groff & Lockwood (2014)	0.068	0.056	0.110	-0.042	0.178	1.070	0.060	0.959	1.194		Not significant
Violent crimes(Robberies)-Drug Treatment Centres , Clutter et al., 2019	0.157	0.383	0.750	-0.593	0.907	1.170		0.553	2.478		Not significant
Violent crimes(Robberies)-Drug Treatment Centres-Lowest value, Haberman & Ratcliffe (2015)	0.162	0.112	0.220	-0.058	0.382	1.175		0.944	1.465		Not significant
<u>Combined Violent crimes (Robberies) - Drug Treatment Centers (3 studies) - Lowest value</u>	0.088	0.049	0.097	-0.009	0.185	1.092		0.991	1.203		Not significant
Violent crimes (Robberies)-Drug Treatment Centres-Highest value, Haberman & Ratcliffe (2015)	0.430	0.110	0.216	0.214	0.646	1.537		1.239	1.907		p<0.001
<u>Combined Violent crimes-Drug Treatment Centers (3 studies) - Highest value</u>	0.216	0.115	0.225	-0.009	0.441	1.241		0.991	1.554		P<0.01
Data for which meta-analysis could not be conducted (Depicted on Forest plot only)											
Property crimes-Drug Treatment Centres, Groff & Lockwood (2014)	0.223	0.896	1.756	-1.533	1.979	1.250	0.070	1.120	1.395		p<0.001
Disorder crimes-Drug Treatment Centres, Groff & Lockwood (2014)	0.247	0.858	1.682	-1.435	1.929	1.280	0.100	1.098	1.492		p<0.01

Data Legend	Provided	Calculated

8. Combined effect sizes that determine influence of Banks & ATMs on crime (Chapter 3, Section 3.3.8)

Authors and Year of Study	Effect size (Coeff)	Std Error of Coeff	95% CI Coeff	LCI	UCI	IRR EXP (Coeff)	Std Error of IRR	EXP (LCI)	EXP (UCI)	z	Significance
Violent crimes (Robberies)-Banks and ATM, Favarin (2018)	0.475	0.1522	0.2983	0.1767	0.7733	1.6080		1.1933	2.1668		p<0.001
Violent crimes(Robberies)-Banks and ATM- late night (Lowest value), Haberman & Ratcliffe (2015)	0.18	0.049	0.0960	0.0840	0.2760	1.1980		1.0876	1.3179		p<0.001
Combined Violent crimes-Banks and ATM (2 studies)- Lowest value	0.208	0.047	0.092	0.1160	0.2990	1.231		0.1082	0.1173		P < 0.001
Violent crimes (Robberies)-Banks and ATM- late night (Lowest value), Haberman & Ratcliffe (2015)	0.296	0.064	0.1254	0.1706	0.4214	1.3440		1.1860	1.5242		p<0.001
Combined Violent crimes-Banks and ATM (2 studies)- Lowest value	0.323	0.059	0.116	0.2070	0.4390	1.381		1.230	1.551		P < 0.001

Data Legend	Provided	Calculated

Appendix 4

a. Search strings and results – systematic literature review

Search Query	Results
Smart CCTV	
"smart cctv" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	24
"connected cctv" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	5
"intelligent cctv" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	28
video surveillance system cctv "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario"	59
"Internet of Surveillance Things" scenario attack	60
surveillance attack scenario security risk threat "cyber attack" OR "cyber threat analysis" OR "attack effect" OR "cascading impact" OR "ripple effect" "smart cctv"	13
"smart cctv" surveillance camera "attack scenario" OR "failure scenario" OR "security assessment" OR "security analysis" OR "threat analysis" OR "threat assessment" OR "cybersecurity risk" OR "Cybersecurity assessment"	48
cctv "reports of attacks"	49
TOTAL for Smart CCTV	239
Smart lighting columns	
"smart streetlight" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	12
"connected streetlight" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	0
"intelligent streetlight" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	2
"smart lighting system" "cascading effects" OR "security scenario" OR "threat analysis" OR "failure scenario" OR "security assessment" OR "threat assessment" OR "risk analysis"	82
cyber attack "security scenario" OR "threat analysis" OR "failure scenario" OR "security assessment" OR "threat assessment" OR "risk analysis" "STREETLIGHT" - traffic -airport -building	14
cyber attack "security scenario" OR "threat analysis" OR "failure scenario" OR "security assessment" OR "threat assessment" OR "risk analysis" "LIGHTING poles" - traffic -airport -building	1
cyber attack "security scenario" OR "threat analysis" OR "failure scenario" OR "security assessment" OR "threat assessment" OR "risk analysis" "SMART LIGHT" - traffic -airport -building	22
cyber attack "security scenario" OR "threat analysis" OR "failure scenario" OR "security assessment" OR "threat assessment" OR "risk analysis" "CONNECTED LIGHT" -traffic -airport -building	2
cyber attack "security scenario" OR "threat analysis" OR "failure scenario" OR "security assessment" OR "threat assessment" OR "risk analysis" "LAMP POST" -traffic -airport -building	3
cyber attack "security scenario" OR "threat analysis" OR "failure scenario" OR "security assessment" OR "threat assessment" OR "risk analysis" "smart LAMP POST" - traffic -airport -building	0
"smart streetlight" "Cybersecurity assessment" OR "cyberthreat analysis" OR "risk assessment"	23
cyber attack "security scenario" OR "threat analysis" OR "failure scenario" OR "security assessment" OR "threat assessment" OR "risk analysis" "street light" -traffic -airport -building	7
TOTAL for Smart lighting columns	181

Smart EV charging	
"smart ev charging" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	48
"smart Electric vehicle charging station" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	3
"smart EVSE" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	5
"smart EVCS" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	6
"smart EV charging" "reports of attacks"	0
"EV Charging Ecosystem" "Security Assessment" OR "Failure Scenario" OR "threat assessment" OR "cybersecurity threat" OR "cybersecurity risk" OR "cyber threat analysis"	96
"smart EVSE" "Security Assessment" OR "cascading effects" OR "Failure Scenario" OR "threat assessment" OR "cybersecurity threat" OR "cybersecurity risk" OR "cyber threat analysis" OR "risk assessment"	4
"smart EVCS" "Security Assessment" OR "cascading effects" OR "Failure Scenario" OR "threat assessment" OR "cybersecurity threat" OR "cybersecurity risk" OR "cyber threat analysis" OR "risk assessment"	5
"smart Electric Vehicle Charging " "Security Assessment" OR "cascading effects" OR "Failure Scenario" OR "threat assessment" OR "cybersecurity threat" OR "cybersecurity risk" OR "cyber threat analysis" -Gumrukchu, Girdhar - NESCOR	72
"EV charging" scenario "cyber-physical threat" OR "security scenario" OR "infrastructure threat model" – Reeh, Caroll	25
Smart EV charging Total	264
Smart bus stop	
"smart bus stop" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	3
"connected bus stop" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	0
"intelligent bus stop" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	0
"smart bus shelter" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	0
"connected bus shelter" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	0
"intelligent bus shelter" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	0
"smart bus stand" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	0
"connected bus stand" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	0
"intelligent bus stand" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	0
"smart bus transit" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	0
"connected bus transit" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	0
"intelligent bus transit" "attack effect" OR "cascading impact" OR "ripple effect" OR "attack scenario" OR "cyber attack" OR "cyber-attack" OR "cyber threat analysis"	0
Queries below were run for all combinations as seen above	
"smart bus top" "report of attacks"	0
"smart bus stop" "cascading effects" OR "security scenario" OR "threat analysis" OR "failure scenario" OR "security assessment" OR "threat assessment" OR "risk analysis"	8
"smart bus stop" Cybersecurity assessment" OR "cyberthreat analysis" OR "risk assessment"	21
TOTAL for smart bus stop	32

- b. Six studies were suggested by the researcher's network and included in the systematic literature review:

Title and author for six studies from grey literature:

1. 'I'm hacked' message left on dozens of defaced Canon IoT security cameras in Japan (Smith, 2018) – Security news by a private organization
2. Tenable Research Advisory: Peekaboo Critical Vulnerability in NUUO Network Video Recorder (Tenable Research, 2018) – Blog run by a private organization
3. Two Arrested in UK for Hacking DC CCTV Cameras Before Trump Inauguration (Hackread, 2017) – News report
4. Surveillance Chess (Bitnik, 2014) – Blog
5. Engineer gets 8 months' jail for hacking into police CCTV cameras at SEA Games 2015 (Hussain, 2016) – News report

Report from a private organization included in systematic literature review:

1. "Resilient Electrical Vehicle Charging: 'REV'" (Sygensys for National Grid ESO, 2022) – private organization project report

Appendix 5

Chapter 5 – Thematic analysis of gaps in the procurement process– section 5.4.2

A. Initial list of Gaps in procurement process to address cyber resilience of connected places

Topic	Gaps
Contract specifications	Lack of sufficient cyber risk management evaluation criteria in procurement frameworks
	Lack of agreed cyber resilience requirements across LA
	Focus is on zero liability to the LAs in the procurement contracts rather than minimal cyber risk exposure
	Lack of assessment of external dependencies (that can help limit a cyber-attack) within the procurement framework and contract specifications
	There is no requirement in the procurement process to check if monitoring systems for connected place ecosystem are independent from the operational connected place systems
	There is no requirement in the procurement process put on CPO to test (dry run) the disaster recovery, service continuity and business continuity plans against full-fledged list of potential cyber-attacks.
	Service performance metrics are built for traditional service operations with quick fix to mechanical faults in mind, not cyber-attacks for connected places
Contract Award	The LAs do not conduct a formal risk assessment to the connected place ecosystem prior to contract award.
	CPO leads on cybersecurity and cyber resilience of smart services rather than the LAs
	NCSC connected place guidelines not reviewed for procurement of smart services
	Accountability of managing security and resilience risks of smart service is outsourced to CPO
Contract management	There are no checks on whether the connected place ecosystem cyber risks are managed by CPO or LA
	The 'right to audit' is not exercised by the LA for EV charging smart service
	CPOs are not required to provide the LA with ongoing cyber threat monitoring reports
	There are no checks on CPO as to whether they are conducting regular threat assessment and are adjusting protections as per change in threat landscape
	Cyber anomalies across operator networks are not analysed to understand the threat to the connected place ecosystem
	CPOs are not assessed for maturity of their cyber security levels during the term of the contract.
	There is lack ongoing assurance mechanism for insider threats within the connected place to prevent hostile countries gaining access to smart services
	LA did not see the need to build any assurance mechanism to check whether CPO is prepared for cyber-attack. Reputational and other dependent risks in the event of cyber-attack are in effect not managed by LA.
	The cyber risk assessments conducted by CPO are IT focussed. They are not assured from the lens of cyber-attack critically disrupting EV charging services, EVs, power grids or any other connected ecosystems

Topic	Gaps
Service management	Resilience tests for a connected place ecosystem are not taken up regularly.
	Recovery planning from cyber-attacks in a connected place ecosystem is not done in a structured manner across the LAs by resilience forums.
	LA are not aware of the incident response team across connected place and planning or review of cyber incidence response, for example, if there is a ransomware attack that spreads across a connected place, how will it be resolved.
	There is no requirement in the procurement process put on CPO to analyse the disaster recovery, service continuity and business continuity plans against full-fledged list of potential cyber-attacks
	Police do not engage upfront to insert security interventions to prevent potential cybercrimes leading to service disruptions.
	Local Resilience forums are not engaged upfront to minimize the risk to connected place in event of cyber-attack on a smart service
Contract Closure	LA and CPOs are not necessarily aware of lessons learnt on cyber resilience in the industry
Approach and capabilities	There is lack of accountability for cyber risks of the connected place ecosystem
	CPO leads on cyber security and makes decisions on what functionalities can be provided with minimal risk rather than the LAs
	The LAs don't conduct a formal cyber risk assessment for the dependencies in the connected place ecosystem prior to contract award.
	Mismatch in ownership of cyber risks of the ecosystem in Government guidelines versus local authority processes
	LA have not considered what skills and training is required for governance of cyber risks of the connected place ecosystem.
	Lack of awareness of implications of a cyber-attack and consequences
	Lack of resources, time, skills, and training to translate high level guidelines into specifications to be included in the bids
	Lack of LA capabilities to be accountable for the cyber risks of smart services as well as connected place ecosystem
	Lack of skilled resources for analysis of procurement guidance for connected place services
	Procurement personnel were not aware of NCSC connected place guidelines
Government support	CPOs assure insider threats for their supply-chain. However, there is a lack of regular checks within the connected place ecosystem to assure that the suppliers that have links with hostile countries do not gain access to smart services.
	Not fully developed or mature Policy and standards
	Lack of specific guidance on how to govern operational cyber risks
	No agreed cyber risk management standards
	Lack of adequate framework of cyber risk audit and assurance
	There is no guideline available from NCSC on audit and assurance of smart services or connected place ecosystem.
	LA procurement professionals unaware of NCSC cybersecurity principles for connected places
	LA needs guidance to identify the gaps that need to be looked at to understand the gaps in their procurement process and develop capabilities for governing them.

Note: LA - Local authority, CPO - Charge point operator

B - Thematic Gap Analysis

Theme 1: Lack of accountability for cyber risk management for the connected ecosystem

Gap: Multiple suppliers in the connected place own the security risk across their smart infrastructure and services. The risks associated with this model of governance are not analysed. LAs are accountable for procuring smart services but are not accountable or liable for the overall cyber risk management of the connected place ecosystem. This results in LAs not being aware of the overall cyber risk exposure and dependencies within the connected place ecosystem.

Barriers: There is a mismatch in ownership of cyber risks of the ecosystem in Government guidelines versus local authority processes. The LAs have traditionally been following the model for the procurement of services in which they are not liable for any incidents. For example, if they provide parking land on lease to a private operator, the LAs are not liable for a parked car being vandalised. This model may not work for digital services in a connected place as the cyber risks, if not managed, can impact CNI and essential services.

Challenges: The LAs do not have the relevant capabilities to take on accountability for the cyber risks of smart services, as well as the connected place ecosystem. As a result, the focus is on stipulating a zero liability on the part of the LAs in their procurement contracts, rather than focussing on reducing the cyber risk exposure. Due to lack of clarity on how cyber-attacks can critically disrupt the grid through an attack on EV charging services, the cyber risk assessments conducted by CPO are IT focussed. They are not assured from the lens of a connected place ecosystem.

Theme 2: Insufficient and inconsistent cyber resilience specifications in CPO contracts

Gap: There are insufficient and inconsistent specifications for cyber-resilience and cyber risk monitoring in CPO contracts across LA. This results in LA not being aware of whether sufficient security measures are being applied and adjusted by the CPOs based on the changing threat landscape. This also exposes LAs to unknown amounts of cyber risk in the connected place ecosystem, even if all suppliers have fulfilled compliance of their individual contracts.

Barriers: Procurement contracts are created for each smart service and LA are not setup to assess cyber risks are formally across multiple procurement contracts. CPO leads on cyber security and makes decisions on what functionalities can be provided with minimal risk, rather than the LAs due to their lack of capabilities. This puts CPO in the position of power. The LAs chase the same set of suppliers and insisting on too many requirements is seen as a roadblock to securing a CPO.

Challenges: There is lack of resources, time, skills, and training provided to the LAs to translate high level guidelines into detailed specifications to be included in bids. There are too many guidelines, which LA find difficult to navigate and standards are yet to mature. The LAs need to understand implications of potential cyber-attacks and consequences of not including the required standards for cyber resilience in the bids.

Theme 3: Lack of Operational Governance by LAs for cyber risks across smart services

Gaps: Service performance metrics reported to LA are not considering digital risks. Additionally, monitoring reports, resilience tests and recovery planning are not done in a structured manner across LA for the ecosystem. This results in lack of understanding of the developing threat landscape for the ecosystem and how prepared the connected place ecosystem is in event of a cyber-attack on a specific smart service. There is no requirement for a CPO to test (dry run) the disaster recovery, service continuity and business continuity plans against a fully-fledged list of potential cyber-attacks. Reputational risks and other dependent risks resulting from a cyber-attack are, in effect, not managed by the LA.

Barriers: LAs are not accountable for the operational risks, nor are they liable for cyber security breaches of services in a connected place ecosystem.

Challenges: LA are not aware of the incident response team across connected place and planning or review of cyber incidence response, for example, if there is a ransomware attack that spreads across a connected place, how will it be resolved. Local Resilience forums and police are not engaged upfront to minimize the risk to connected place in event of cyber-attack on a smart service. Resilience tests for a connected place ecosystem are not taken up regularly.

Theme 4: Lack of Assurance by The LAs for cyber risks for smart services, as well as the ecosystem

Gaps: Lack of ongoing audit and assurance for cyber risks during the term of the contract results in lack of cyber security benchmarks. Additionally, LA do not have visibility of whether CPO maintains appropriate and proportionate security levels for their operations. LA depend on procurement frameworks and do not have visibility on how CPO manages risks such as insider threats with links to hostile countries who could gain access to the smart services in the ecosystem.

Barriers: Analysing the outward dependencies that can help spread or limit a cyber-attack, due to the connected nature of infrastructure and services within the connected place ecosystem, is not prescribed within the procurement process (for smart services or legacy services that are being upgraded to smart services). LAs did not see the need to build any assurance mechanism in order to check whether a CPO is prepared for a cyber-attack or is regularly managing the continuously developing operational security risks. The reason is that this aspect is essential to the CPO's business, so the LAs don't see the need to intervene. The attitudes to cyber security are relaxed, as it is not seen as being a high probability or high impact risk. This is because LAs haven't experienced or heard of any large-scale cyber-attack on EV charging impacting CNI. There is lack ongoing assurance mechanism for insider threats within the connected place to prevent hostile countries gaining access to smart services as the supply-chain is an internal matter for the CPO.

Challenges: There is lack of skills, expertise, and capabilities to i) understand the context of cyber risks across systems and services, ii) analyse the dependencies and impacts in the connected place ecosystem, and iii) collate guidance in procurement frameworks. Hence, LAs have not verified the level of risk and are not aware of cybercrime scenarios, the threat landscape, and cyber risks to national essential services through a cyber-attack on smart services such as EV charging.

Theme 5: Inadequate skilled resources and capabilities in the LAs

Lack of skilled resources within the LA results in high-level guidance (such as NCSC connected place guidelines) not absorbed by traditional procurement functions and CPO being in position of power.

Barriers: Due to the lack of risk structure across organizational limitations, LA and CPOs are not necessarily aware of lessons learnt on cyber resilience in the industry. In traditional functions such as procurement, there is less awareness or ownership to implement NCSC connected place guidelines which are not mandated. There isn't a fully developed or mature Policy and standards, guidance on how to govern operational cyber risks and cyber risk management standards. LA needs guidance to identify the gaps that need to be looked at to understand the gaps in their procurement process and develop capabilities for governing them.

Challenges: Due to lack of skills, CPOs are not assessed for maturity of their cyber security levels during the term of the contract. CPO leads on cyber security and makes decisions on what functionalities can be provided with minimal risk rather than the LAs. Due to Lack of awareness of implications of a cyber-attack and consequences, LA have not considered what skills and training is required for governance of cyber risks of the connected place ecosystem.

LA - Local authority, CPO - Charge point operator