Leiden University

The Cyber Risk and Vulnerability of Smart City

A Case Study of Smart City Projects in Eindhoven (the Netherlands)

Supervisor: Dr Vlad Niculescu-Dincă

Second Reader: Dr Els de Busser

Monique Xueying Chen

Master Thesis

MSc Crisis and Security Management

S1933582

word count: 22390

Abstract

Smart city transforms the traditional urban infrastructure into a network of interconnected physical and digital systems in order to address the challenges of urbanization. Beyond that, some smart cities are applying open innovation principles aiming to establish an innovation hub where public organizations, private companies, knowledge institutions and the citizens co-create the city. Smart city with open innovation features embraces open data standards and multi-stakeholder development model. Meanwhile, the use of smart city technologies and the openness of a smart city introduce a new paradox of cyber risk and vulnerability, presenting challenges to the cybersecurity of smart city. Consequently, smart city is concerned with cyber insecurity and needs to present adequate measures to prevent and mitigate the cyber risk and vulnerability.

The aim of this research is to conduct a holistic assessment of cybersecurity measures against cyber risk and vulnerability in the smart city projects in Eindhoven with open innovation characteristics. Through the analysis of interviews and documents, this research strives to conclude what cyber risks and vulnerabilities are concerned by the smart city projects when applying open innovation principles, as well as the measures and policies taken against cyber insecurity. By testing the empirical data against the theoretical framework, this research aims to highlight the particular focuses and solutions presented in this holistic case study. In turn, this research will enrich the empirical inventory of smart city cybersecurity measures and contribute to the body of knowledge of cyber risk and vulnerabilities.

The result of the research suggests that Eindhoven smart city projects make the privacy concern and data (in)security the priorities in cybersecurity policymaking. The projects propose solutions of multi-stakeholder cooperation, privacy by design, as well as learning by doing model which is beyond the scope of the theoretical framework. However, using a learning by doing model, living labs or pilots in the early stage concentrate more effort on testing functions than maintaining cybersecurity. The projects show different level of emphasis on cybersecurity due to being at different stages of development.

Keywords: smart city, cybersecurity, risk and vulnerability, open innovation, privacy

Table of Contents

Chapter 1 Introduction

1.1 Smart City

The phenomenon of smart city development is an effort to address the urban problems caused by rapid urbanization around the world (Batty et al., 2012). Throughout human history, cities have developed into more and more compressed living spaces where people can connect resources, wealth and ideas easily and efficiently (Townsend, 2013, p. 1). Cities have always attracted people as a symbol of improved living quality and promising opportunities which rural areas cannot provide. Global urbanization went through the flourishing during the twentieth century and has reached a historical threshold. Today, 4.2 billion accounts for the urban population of the world, in contrast to 751 million in 1950 (UN, 2018b). United Nations (UN) predicts that the urban population will expand to 6.7 billion by 2050, taking up 68% of the world population (UN, 2018a). The high development of urbanization is putting tremendous pressure on the management and sustainability of the urban areas. Modern societies are dealing with serious "urban diseases", such as energy shortage, environmental change, traffic congestion, and the shortage of space (Neirotti, De Marco, Cagliano, Mangano, & Scorrano, 2014). These urban issues are sometimes unintended new variations of traditional urban problems, namely rapid population increases, increasing criminal risks, inequality of resources and environmental externalities (Kitchin & Dodge, 2017; Townsend, 2013).

In the search for the solution to the challenges of growth and the "urban diseases", smart city is introduced as a technological solution to counter and manage these issues of urban resilience and sustainability (Coe, Paquet, & Roy, 2001; Hollands, 2008). Smart cities take advantage of communication and connection capabilities sewn into the cities' infrastructures to optimize urban services, such as Wi-Fi connections, street cameras and traffic sensors. The Information and Computing Technologies (ICTs), big data and the appliances of Internet of Things (IoTs) are changing urban lifestyle. These new technologies enable innovative ways of delivering public services and solving urban challenges (Shen, Huang, Wong, Liao, & Lou, 2018). As a result, public services such as public safety, health, and social benefits, traffic management, etc. are being reformed towards smart systems. Smart cities are introduced as connected urban spaces that deliver efficient and sustainable services to residents by applying new technologies to increase the connectivity and the depth of data use (Nam & Pardo, 2011; Neirotti et al., 2014).

Nevertheless, the definition of smart city is under dispute. By some researchers, smart city is recognized as a combination of physical infrastructure and technology in urban systems (Mohanty, Choppali, & Kougianos, 2016). Many scholars stress the aim to improve life quality as the key feature of smart city concept, instead of the smart city technology innovation (Cerrudo, 2015; Dirks & Keeling, 2009; Elmaghraby & Losavio, 2014), whereas other researchers emphasize the smartness and connectedness of the urban space (Kitchin, 2014b). Smart city is also often described as an efficient way to optimize the resources of an urban area, in order to increase the effectiveness of processes in every field of its functioning (Lacinák & Ristvej, 2017). The conceptualization of smart city is an evolving process where new features are constantly added to the discussion. One notable concept of smart city is an open innovation hub which means that smart city tailor-makes its functions according to the input of citizens (Elmaghraby & Losavio, 2014). Bearing this in mind, the concept of smart city needs to be redefined with additional features such as knowledge hub and innovation center (Paskaleva, 2011), which will be addressed in detail in 2.1.1.

It is important to note that even though smart city seems to provide benefits to improve urban life quality, smart city also opens up the gateways to new forms of cybersecurity vulnerability and risk compared to traditional cities. New variances of security risks are generated by connecting the urban systems through smart city technologies, such as software bugs, data collection and analysis errors, viruses, malicious hacks, or terrorist cyberattacks. Smart city projects are exposed to a complex and diverse set of cyber risk and vulnerabilities, whereas a single cybersecurity threat may put the entire project at risk (Khatoun & Zeadally, 2016). Under the guise of digital computation, the motivations of traditional crime, such as fraud, vandalism, theft, and extortion still threaten the smart city systems (Schneier, 2017b). The burgeoning literature has voiced the significance of considering the cyber risk and vulnerability when wiring the city with networked computation. These risks include that strongly coupled systems are prone to software bugs, network viruses, malicious attacks, and data errors (Batty et al., 2012; Kitchin & Dodge, 2011; Townsend, 2013). ICT and regenerated urban problems form a paradox creating security concerns which are largely being underestimated (Kitchin & Dodge, 2017). Meanwhile, the consequences of such an attack could be devastating. For example, a software bug of a power grid in north-east USA in August 2003 resulted in a blackout affecting ten million people and ten deaths from fires and accidents (Beatty, Phelps, Rohner, & Weisfuse, 2006). Therefore, in order to build sustainable

and efficient smart cities that truly serves its purpose of providing improved life quality, it is necessary to investigate and assess the cybersecurity of a smart city.

Previous literature pointed out several aspects wherein the effort to address the cybersecurity of smart city should be made. The first is regarding the governance perspective of smart city development, namely, policymaking and cooperation among stakeholders. This is pointed out in the literature of smart city cybersecurity that it is crucial to ensure a functional and secured smart city by adapting the policymaking to the impacts of smart city technologies (Castelnovo, Misuraca, & Savoldelli, 2016). The second aspect is the suggestion of such a research to adopt a holistic approach, because it is more valuable to gain a contextual and in-depth empirical understanding of smart city (Castelnovo, Misuraca, & Savoldelli, 2016; Mattoni, Gugliermetti, & Bisegna, 2015). The third aspect of research effort should be paid to smart city with open innovation characteristics which is still relatively new to the smart city discussion (Elmaghraby & Losavio, 2014; Schaffers et al., 2011). Elmaghraby and Losavio (2014) introduced the merging phenomenon of cities adopting open innovation where the citizens are considered the center of the city's smart initiatives. Open innovation is an important experiment of becoming more sustainable, open and user-driven smart city design, by means of living lab method and a citizen-centric bottom-up approach (Almirall, Lee, & Wareham, 2012; Schaffers et al., 2011). They often have multiple stakeholders that are intensively involved in the process of decision-making and implementation. Of the partners, private companies are usually engaged by providing hardware or software services (Elmaghraby & Losavio, 2014). It is also important to note that open innovation provides the ground to grow a knowledge hub and innovation center. Thus, it attracts technology companies, research facilities and talents to the city, which in turn, boosts the innovation of the smart city in long-term (Schaffers et al., 2011). It is becoming more necessary to look into the development of this new smart city type as more cities are embracing open innovation (Paskaleva, 2011). It is, therefore, relevant to contribute to the research of smart city with open innovation characteristics, by examining the cybersecurity risk and vulnerabilities that it presents.

To answer the problems outlined and to follow the research opportunities pointed out in the literature, this thesis adopts an explanatory theory testing design. By testing a theoretical framework with a case study, this thesis aims to contribute to the empirical knowledge of smart city cyber risk and vulnerability. In order to do so, a literature review will be made to form the

theoretical framework. Guided by the theoretical framework, this research gathers in-depth holistic empirical data to illustrate the cybersecurity concerns and the policies applied in the development and implementation of smart city projects. More specifically, it highlights the cybersecurity concerns and measures bearing open innovation in mind. By doing so, this research tests and improves the theoretical framework of smart city cyber risk and vulnerability by examining the policies to prevent and mitigate the cyber risks and vulnerabilities.

1.2 Research Question and Sub-Questions

In light of the introduction above, the central research question that guides this research is:

> **How do smart city projects with open innovation characteristics prevent and mitigate cyber risk and vulnerability?**

In order to answer the research question, the following sub-questions need to be addressed:

> What risks and vulnerabilities are concerned by Eindhoven smart city projects?
>
> What policies and measures do Eindhoven smart city projects apply to prevent or mitigate cyber risks and vulnerabilities?

1.3 Academic and Societal Relevance

Contrasting the high-speed development of smart city technologies and the enthusiasm of smart city projects, the cybersecurity of smart city technologies is often ignored or underrated. This research has both academic and societal significance in response to the attention to cyber risk and vulnerabilities in smart cities. The academic relevance of this research lies in its effort to contribute to the existing literature by constructing a theoretical framework. First, through literature research, this research will analyze, assess and learn from previous research on smart city cybersecurity to build the primary theoretical framework. Then, this research will improve the theoretical framework through empirical research and case study. Previous research has pointed out that building a theoretical framework through a case study is especially appropriate in new and untested studies. Through an empirical case study, the theoretical framework will be testable and empirically valid (Eisenhardt, 1989). Previous research in a smart city called for a holistic approach in smart city research (Castelnovo et al., 2016; Mattoni et al., 2015). This study adds updated empirical data detailed to a city context. Analysis situated in a specific city context will offer insights that will allow future research to incorporate the empirical data. Importantly, drawing

from the theoretical framework of smart city cyber risks and vulnerabilities, this research seeks to gain contextual insight and test the theory with current smart city cybersecurity policies. This theory testing will contribute to the development of a comprehensive theoretical framework that would help to assess the cybersecurity policies in smart cities as there is currently no unified model for it. Furthermore, this thesis will base on previous smart city cybersecurity research, furthering the understanding of policies to mitigate risk and vulnerabilities post by a smart city.

The relevance of this study to the field of Crisis and Security Management lies at the significance of cybersecurity in securitization study. Smart city is a buzzword that attracts much attention from governments, technology vendors, and citizens driving municipalities around the globe to explore digital transformation projects. Researcher are growing more and more concerned with the cyber resilience of living in a smart urban environment with interconnected gadgets, sensors and cameras everywhere (Elmaghraby & Losavio, 2014; Kitchin & Dodge, 2017). This concern creates an urgent need to assess the main cybersecurity policies regarding what cyber risks and vulnerabilities are being well managed and what are given less attention.

Cyberattacks on smart city infrastructure or breach of data through interconnected parts of the smart city made the society realize that cyber vulnerabilities exist and impact deeply in civil lives (Alba, 2015). Thus, this research has its societal relevance as it is vital to evaluate the cybersecurity policies of the smart cities, providing the policymakers a realistic sketch of the cyber resilience of Eindhoven. The findings, in turn, empowers the city with a possible framework to improve the development of the smart city. Conducting this research could raise awareness among citizens of cybersecurity in the engagement with smart city development and contribute to overall structural thinking of cyber resilience of building smart cities. Furthermore, Dutch cities are striving to innovate easier and faster through the Smart City StarterK!t, which consists of a combination of policy and technological instruments. The kit was developed by the Dutch Institute for Technology Safety & Security (DITSS), whose foundation lies in the Eindhoven Living Lab. The experience of smart city Eindhoven is shared through this kit to save other municipalities valuable development time while smoothing the transition to a smart city. The result of this research will contribute to the development of the Smart City StarterK!t, presenting the value of reference to the development of other smart city projects.

1.4 Reading Guide

This thesis is constructed as follows: An introduction to the research topic and the research questions is given in Chapter 1. Chapter 2 addresses the body of knowledge in the cyber risk and vulnerabilities in smart city. Chapter 3 presents the methodological structure and the analytical framework of this research. Chapter 4 conducts the analysis of cybersecurity policies applied in a case study. Chapter 5 concludes the result of the research. Chapter 6 discusses the findings and proposes suggestions for future research.

Chapter 2 Theoretical Framework

2.1 Conceptualization

In order to form a clear theoretical framework of smart city cyber risk and vulnerability, chapter 2.1 will be dedicated to defining the relevant concepts that will be frequently discussed in the rest of the research. The conceptualization of smart city, cyber risk and vulnerability and cyberattack will be defined based on previous research and the research focus of this thesis.

2.1.1 Smart city

It is commonly identified in research that smart cities are the ones that rise to the urbanization challenges with smart solutions (Nam & Pardo, 2011) which is rather flexibly defined. The conceptualization of smart city is developed in various disciplines, baring different perspectives in previous literature. Smart city notion can be elaborated through a taxonomy of its various application domains, namely, mobility, building and living space, transport, and economy, etc. The diffusion of smart city is also explored within a certain geographical and economic domain. This point of view reveals that the development patterns of smart cities largely depend on their local context factors. A typical example is Chinese smart cities which prioritizes balancing the supply and demand of urban infrastructure, in face of the challenges posed by rapid urban population growth. Smart city technologies are being applied to monitor where more relevant infrastructure is needed, instead of aiming at better social service for overall civilians (Wu, Zhang, Shen, Mo, & Peng, 2018). Although, a globally shared conceptualization of smart city is hard to identify, this

conceptualization categorizes previous smart city concepts oriented by four focuses: technology, economic, urban services, and knowledge hub of innovation.

The following section will elaborate on each focus in order to land on one definition for this research. The first focus is technology, the intelligence of a city is what makes it "smart", which means that the definition of a smart city emphasizes that ICT is a key enabler of smart city design. Smart city is presented as a citywide control system with ICT systems as the central nervous organ that collects data from diverse sources in the city, such as security cameras and traffic lights. Intelligent Community Forum (ICF) annually assesses intelligent communities by its success in five factors: broadband connectivity, knowledge workforce, digital inclusion, innovation, and marketing and advocacy (Nam & Pardo, 2011, p. 283). Of which, three factors are technology focused. It is believed that in order to achieve innovative and transformational development, an international-level information infrastructure system, an effective information-sensing and intelligence application system, a next-generation IT industry, and a trusted and reliable regional information security system are required (Mohanty et al., 2016). This conceptualization is in line with some literature as well. Caragliu, Del Bo, and Nijkamp (2009) summarized a smart city as a synthesis of hard infrastructure (or physical capital) with the availability and quality of knowledge communication and social infrastructure.

The second focus of smart city conceptualization is smart city as a business model. This perspective of conceptualization adapts an economic perspective that smart city aims to maximize the efficiency of resource management. Foregoers of smart city initiative have obtained a series of achievements focusing on the economic perspective. One of the earliest and frequently quoted definition by International Business Machine (IBM) describes smart city as a city that could "maximize the payment with limited input of resources by the use of techniques to improve urban services in multiple aspects including civilian, business, transportation, communication, water, sources and other urban systems" (Dirks & Keeling, 2009). Such definition is typically adopted in the economic domain focusing on the optimal efficiency. The economic focus is also suggested by some scholars that a smart city is one that increases the effectiveness of processes in every field of its functioning (Lacinák & Ristvej, 2017). Policymakers of Europe stress that it is highly relevant and necessary to harness the power of smart cities for more effective competition with rival global economies (Manville et al., 2014, p. 19).

The third focus of smart city conceptualization lies with smart city as a concept of urban lifestyle. It comes from the view of city dwellers, describing smart city as a more convenient, safe, healthy, and sustainable living environment comparing to the traditional urban space. Some researchers view a smart city as "a city seeking to address public issues via ICT-based solutions on the basis of a multi-stakeholder, municipally based partnership" (Manville et al., 2014). It is, thus, a place where traditional networks and services are made more flexible, efficient, and sustainable with the use of information, digital and telecommunication technologies, to improve its operations for the benefit of its inhabitants. Smart cities are greener, safer, faster and friendlier (Mohanty, Choppali, & Kougianos, 2016). Simply put by Cerrudo (2015), it is a city that uses technology to automate and improve city services, making citizens' lives better.

The latest focus of smart city definition is its purpose of serving as a knowledge hub, where innovation takes center stage (Batty et al., 2012). Much like how tech giants are gathered in hubs such as Silicon Valley, companies and talented people are lured to smart cities, creating internet-driven hubs for innovation. "Ideas naturally exchange and cooperate between companies in that cluster," said Kenneth Fredriksen, vice president of Huawei's Central European and Nordic region. This pool of talent created by smart city phenomenon is pursued by EU's upcoming 'Horizon 2020' research funding programme. It seeks to promote clusters by encouraging large consortiums of large companies, research facilities, and small business to co-exist in such hubs to advance innovation and economy (EurActiv, 2013).

Two considerations are made to land on one conceptualization of smart city for this research. One consideration is to consider all the four focuses listed above, the other is to consider both the technological and organizational aspects of a smart city. It is important to consider all the focuses listed above for the reason that smart cities do not have one focus exclusively but a combination of focuses. For a smart city with open innovation features, it focuses on creating a providing improved living quality to the citizens, but also on creating an innovation hub where more stakeholders are attracted to generate long-term economic growth (Schaffers et al., 2011; Smith, 2018). It is necessary to include both the technological and organizational aspects of a smart city in the discussion of cybersecurity since a chain is only as strong as its weakest link. Smart city technologies are made possible with organizational architecture, whereas the policymaking

facilitates the successful implementation of smart city technologies. Therefore, it is significant to consider both aspects in smart city research regarding cybersecurity.

Based on the above literature and considerations, this research forms the definition of smart city as following: Smart City is an urban environment that is enabled and enhanced by ICTs, IoTs and big data technology, which integrates technology and urban environment to increase the safety, effectiveness, and efficiency of its functions, aiming to achieve sustainable development, improved life quality and open innovation.

There are generally five main components that are required in a smart city: modern information and communication technologies, buildings, utilities and infrastructure, transportation and traffic management and the city itself. Smart city programs implemented in these components is best summarized guided by Eindhoven University of Technology (TU/e) Smart Cities Program: Smart buildings and hybrid energy systems: Smart buildings & hybrid energy systems; Smart mobility; Smart urban space; Urban data and data platforms; Smart society; Innovation ecosystems (AlDairi & Tawalbeh, 2017; Cerrudo, 2015; Lacinák & Ristvej, 2017; TU/e, 2019). Smart buildings & hybrid energy systems, Smart mobility, and Smart urban space are the three most common application areas in cities transitioning to smart cities. Smart buildings & hybrid energy systems provide a healthy and sustainable living environment for citizens. Smart mobility provides more efficient, inclusive and safer mobility and logistic systems with people's perspective in design. Smart urban spaces enable a multi-functional urban area where citizens enjoy engaged services. Urban data and data platforms together with smart society are two cross-cutting enablers of change. It is only with the aid of big data and suitable platforms, a smart society with the healthy economic climate and strong social networks can be achieved. Moreover, innovation ecosystems are key to success, being major drivers to facilitate citizens, industry, and knowledge in an innovation structure (TU/e, 2019).

2.1.2 Cyber risk and vulnerability

This research discusses the cyber (in)security of a smart city by addressing its cyber risk and vulnerability. The definition of risk and vulnerability adopts the concepts stated by Aven (2017). Risk is defined as "the combination of possible consequences and associated uncertainties (uncertainties of what will be the consequences)" whereas vulnerability is defined as "the combination of possible consequences and associated uncertainties are given a source" (Aven,

2007). Risk and vulnerability analysis method suggest that the term refers to only the feature or aspect of the system that is judged to give high vulnerability (Aven, 2007). Meanwhile, this research will not detail the vulnerabilities and risks from societal aspect or natural disasters, such as political turbulence or flooding. Even though they too can be destructive to a smart city system, this research will focus on the most relevant risk and vulnerability concern of smart city that can be prevented or mitigated, such as risk of cyberattack on IoTs. Thus, cyber risk and vulnerability is defined as weaknesses of a system enabled by automatic computation and the potential consequences of the weaknesses.

2.1.3 Cyberattack

This research focuses on cybersecurity of the smart city, including the vulnerabilities and risks in the face of the threats of cyberattacks. Cyberattack is defined as "alter, disrupt, deceive, degrade, or destroy computer systems and networks or the information and/or programs resident in or transiting these systems or networks" (Owens, Dam, & Lin, 2009). There are commonly acknowledged three types of cyberattacks against operational systems: availability attacks, confidentiality attacks, and integrity attacks (Kitchin & Dodge, 2017; Schneier, 2017a). Availability attacks target the operationality of a system, aiming to disrupt or close a system. Attackers can use viruses to delete data or encrypt data for ransom. Hospitals have paid tens of thousands of dollars in order to regain access to their ransomware encrypted critical medical files (Harkins & Freed, 2018). Confidentiality attacks try to obtain information from a system, which Schneier (2017a) argues are the most concerned attacks in general. Confidentiality attacks compromise the user's privacy, data security, causing possible misuse of the data. Integrity attacks seek to alter information, deceive users, transform the intended use of a system, or plant malware and viruses without being detected. Attackers are not always trained professionals, government-funded cyberattack units and a "script kiddie"[1] propagating trojans found on the dark web (Mead, Hough, & Stehney II, 2006) both can throw a wrecking ball to a computer system. A cyberattack can be driven by financial gains (e.g. business espionage), motivation to cause panic and anxiety (e.g. organized crime and terrorist group), etc.

[1] A script kiddie refers to a person who uses existing computer scripts or codes to hack into computers, lacking the expertise to write their own.

2.2 Literature review

2.2.1 Cyber Risk and Vulnerability Theory of Smart Cities

As a means to enhance the urban life quality, smart city is increasingly popular in the agendas of policymakers (Batty et al., 2012). Pointed out by Batty et al. (2012), cities are becoming strongly interconnected systems that generate complicated dynamics that need to be understood. Smart city technologies, however, come with its cyber risks and vulnerabilities which less attention has been given to (Castelnovo et al., 2016; Elmaghraby & Losavio, 2014). Some researchers discussed the possible solutions to anticipate and counter the risk, uncertainty, and hazard in the smart city. Batty et al. (2012) proposed to introduce new technologies that can outsmart the smart city (Batty et al., 2012). By doing so, the technologies will be advanced enough to anticipate and outsmart the security challenges of smart cities today. Whereas others argue that technological solution cannot by itself resolve cyber insecurity issues. It is crucial to understand the cyber risk and vulnerability posed by the information technology itself. This means that a realistic and practical examination of the cyber risk and vulnerability of the smart city data and technology is the necessary strong base for cybersecurity (Baig et al., 2017; Jin, Gubbi, Marusic, & Palaniswami, 2014). An assessment of a current smart city system cannot be achieved through brute force risk assessment, for the reason that it is beyond the computing abilities to assess all the devices and the types of agents involved in the system. Therefore, the risk and vulnerability of a smart city should be assessed through two steps. First, capture the range and correlation of the driving factors in the smart city system. Second, search mechanisms which can identify how widely applied and how interconnected the central functions of the systems are (Batty et al., 2012). Additional to understanding the risk and vulnerabilities from the technologies, Batty et al. (2012) point out that an informed understanding of risk and vulnerability in smart cities also requires taking new collective approaches to decision-making into account.

To sum, previous research stresses the importance of researching the cybersecurity of smart city technologies as well as smart city governance approaches, in order to better understand the cyber risk and vulnerability in smart cities. Therefore, a valid smart city cyber risk and vulnerability theoretical framework need to reflect both research aspects. To do so, a literature review of the current cybersecurity research of smart cities is conducted in the following part of 2.1.1, to construct a systematic theoretical framework. Following the research focus of addressing both

technological and organizational aspects, this literature review first outlines research that focuses on cybersecurity of smart city technologies, then summarizes the research focus of cybersecurity governance.

This section will discuss the cyber risk and vulnerability focused on cybersecurity of smart city technologies. When analyzing cyber risk and vulnerability from a technology perspective, much attention is given to cybersecurity of IoT (Baig et al., 2017; Bekara, 2014; Jin et al., 2014). Jin et al. (2014) pointed out that when the smart city system is enabled by combining the physical infrastructure and IoT technology, it faces several security issues. The first is the risk of impersonation/identity spoofing. It refers to the risk of the unauthorized user taking the identity of a legitimate part of the smart city system. By this way of attacking, it is possible that someone spoofs the identity of others to be anonymized or to avoid payment. Secondly, an attacker can eavesdrop the data exchange through public communication infrastructure, which compromises the privacy of users. The third cybersecurity concern is data tempering, which results in false data registered in the system. An attacker or an employee with malicious intent may gain unauthorized access to manipulate or damage the remotely deployed devices, such as sensors or meters. As a result, it causes the fourth cybersecurity issue: authorization and control access issues. The fifth issue is the privacy concern where personal data of users could be compromised. It is possible to analyze the fine-grained data to peep into the lifestyle or habits of a person. It is against the privacy law, as well as possibly harmful to the data owner's personal safety. The sixth concern is compromising and malicious code, which is a security concern of software security of IoT. IoT system is made possible by multi-level, interconnected devices. Massively deployed devices such as sensors are not always non-tamper-resistant devices, making them vulnerable to software infection or malicious code infection. Lastly, availability and issues are concerned by the author. With an example of smart grid, Bekara (2014) illustrated the possibility of targeting integrated ICT. If done in the vital parts of the grid, the damage would be substantial. This cyber insecurity is newly appeared in smart grid due to the necessary connection of ICT assets (electricity meters, substations, etc.) to the central system.

The research of Bekara (2014) discussed the smart city cyber risk and vulnerability in detail, including the perspective of data safety and privacy. However, it was done by only examining the cybersecurity of IoT within one smart city function of smart grid. Smart city projects are often

designed with the application of IoT, but not limited to the use of IoT (Nam & Pardo, 2011). The functions of smart city includes but not limited to smart buildings and hybrid energy systems: smart buildings & hybrid energy systems; smart mobility; smart urban space; urban data and data platforms; smart society and innovation ecosystems (AlDairi & Tawalbeh, 2017; Cerrudo, 2015; Lacinák & Ristvej, 2017; TU/e, 2019) It is thus necessary to take other smart city technologies and functions into consideration when composing a theoretical framework of smart city cyber risk and vulnerability.

Kitchin & Dodge (2017) provided a comprehensive theory of smart city risk and vulnerability in the technology perspective. The theory looked beyond one smart city technology or function. It examined the security vulnerabilities and risks of smart cities resulted from the common smart city technologies. It focused on the cyber insecurity of the possibilities of hacking, disruption, and criminal activities. Compared to the research of Bekara (2014), Kitchin & Dodge (2017) did not limit the focus on IoT technology. This theory included the cybersecurity of software and hardware as well as their interconnection in smart city systems. It also takes public and private cooperation into consideration. It summarized the vulnerabilities in five dimensions: 1). software and data encryption vulnerability 2). system and maintenance insecurity 3). the risk from interdependencies and complex attack surfaces and 4). cascade effects on cyberattack and 5). Human error. The following paragraphs will elaborate on each of the dimensions by Kitchin & Dodge (2017).

First, weak software security and data encryption. The most concerning threat outlined by Kitchin & Dodge (2017) in software and encryption is zero-day exploits for network viruses and malware etc. Zero-day refers to the day between the vulnerability is known and the first day of the attack (Bilge & Dumitra, 2012). Zero-day exploits are yet undiscovered or unrealized vulnerabilities, therefore, also yet no existing patch is offered. Kitchin & Dodge (2017) explained the reasons for this concern. To start with, every 1,000 lines of code can generally have on average 30 errors or bugs (Li, Shaw, Herbsleb, Ray, & Santhanam, 2004). Developers also indicated an industry average of developers that there are about 15 to 50 errors per 1000 lines of delivered code (Mayer, 2012). It is reasonable that a large system such as a smart city design with millions of lines of code must contain an undeniable amount of errors resulting in potential zero-day exploits. Furthermore, many smart city systems have minimal security built in. Many vendors implement little if no encryption, intensifying this concern (Cerrudo, 2015). Moreover, many smart city technologies,

especially devices on IoT are released to the market without proper testing. The security community struggles to test more technologies applied to smart cities due to their high price and exclusivity to the government or specific users (Cerrudo, 2015).

The second vulnerability addressed is system and maintenance insecurity. As previously mentioned, the smart city system is enabled by interconnected devices and the development of the system is often not conducted in one concentrated period of time. Smart cities often need to layer new technologies onto a previous existing infrastructure that applies much older technologies and software. A software launched decades ago is likely to have not been updated for a while. Some old technologies even no longer have the capability to be mitigated to newer systems (Cerrudo, 2015). Kitchin & Dodge (2017) pointed out that this type of vulnerability can create forever-day exploits. In contrast to zero-day exploits, forever-day exploits target holes in legacy systems that are no longer supported nor can be patched by manufactures (Townsend, 2013, p. 269).

Risks from interdependencies and complex attack surfaces constitute the third vulnerability concern that the large scale of smart city systems making it difficult to ensure security on all components. Smart devices such as smart meters and IoT devices that are located in physically insecure locations pose security concerns. For the reason that the exposed devices create numerous entry points that can be exploited by an adversary (Jokar, Arianpoo, & Leung, 2016). This concern manifests in two aspects, one of which being the security risks exposed by the components of the system. Another aspect of risk comes from linking the components to other systems. In October 2016, the DoS attacks that brought big websites like Reddit and Twitter offline were enabled by exploiting the vulnerabilities in devices like webcams and digital video recorders (BBC, 2016). Furthermore, the interdependencies between systems and software determine the complexity of maintaining security. Because there is no agreed upon architectures for building IoT systems, interconnected devices could be using a different level of encryptions with various communication protocols. When the systems cobble, the chain is only as strong as the weakest link (Sarma, 2015). Moreover, the complexity of the system increases the chance of human error and the number of potential bugs. Above aspects make the establishment of a smart city threat model to mitigate security risks important yet difficult (Cerrudo, 2015).

The fourth vulnerability is cascade effects. A cyberattack on one entity of the smart city can cascade into other entities because of their cloud connection or Software as a Service (SaaS)

solutions (Cerrudo, 2015). Vulnerability assessment needs to take the implications of SaaS allowing attackers to hack one service provider then attack many cities into account.

The last but not the least, the vulnerability resulted by human error and deliberate malfeasance of disgruntled (ex)employees. Human error is unintended mistakes, in forms of weak passwords, opening phishing emails or spreading viruses, neglecting software updates, installing the incorrect configuration etc. (Cerrudo, 2015; Elmaghraby & Losavio, 2014). On the other hand, malicious intentions by attackers can sabotage the integrity of the system with insider advantages (Kitchin & Dodge, 2017). This consequence of this dimension of risk and vulnerability is also detailed in other research. For example, the compromise of timely data delivery due to 1) a Denial of Service (DoS) attack and 2) an attack targeting vulnerabilities found in protocol stacks that are applied in the smart system components (Lu, Lu, Wang, & Wang, 2010). Timely data delivery and exchange between interconnected systems are essential to successful operations of some particular smart city systems, such as traffic management, crowd management, and smart grid. untimely delivery of data in traffic management will result in drivers not being timely informed of road situations or speeding drivers escaping the penalty. An alarm of a detected street fight will delay the reaction time of the law enforcement, compromising the efficiency of crowd management. Similar delay of an alarming situation in the energy grid system can even lead to the blackout of a city. The Northeast Blackout in 2003 is a good example (Andersson et al., 2005).

These dimensions are tangled with the challenges of multi-stakeholder dynamic, urban management pressure, and a lack of competition and regulation in the smart city technology market. Multi-stakeholder practice in smart city development challenges system management and problem attribution. As previously discussed, the management of a smart city is not a one-stop shop. End-to-end security is not tested or managed by a central security team. As a result, when a security risk is detected, the provider or the manufacturer must take the responsibility of patching the bug. However, it is often challenging or impossible to hold one end responsible if the attribution of the problem cannot be clearly determined. The pressure to keep up with the smart city development and urban management challenges also generate security concerns. Kitchin & Dodge (2017) elaborated the concerns in this respect with following arguments. First, under-investment in infrastructure compels a lack of maintenance and over-reliance on the legacy systems enhancing system and maintenance insecurity. Many municipalities still operate on the system from the 90s

or even earlier. Second, the salary level in the most public sector makes it harder to recruit and retain IT staff with the skill set necessary for proper implementation and maintains of the complex smart city system. It means that it is challenging to form a team of security and IT experts that can ongoingly commit to monitoring and enhancing the smart city security. Less funding in human resource also decreases the chance of advanced security training for employees who are involved in the daily running of smart city technologies. Kitchin & Dodge (2017) and Cerrude (2015) promote that any smart city project should employ a "Chief Information Officer" (CIO) and "Computer Emergency Response Teams" (CERTs) as dedicated leadership and personnel. However, a lack of funding might stop a project from forming these teams. As a result, it hinders security by increasing the risk of human error. Third, largely contracted and outsourced services deskill the core capacities in the public sector (Kitchin & Dodge, 2017) and create distributed accountability. In turn, it erodes the risks from interdependencies and complex attack surfaces, making coordination more difficult to achieve when an attack occurs. Forth, a lack of cross-function assessment and validation of smart city vendors can cause destructive consequences to the system by enlarging the risks of software and data encryption vulnerability, risks from interdependencies and complex attack surfaces, and risks of human error. Many vendors oversell their promise of smart city technologies but provide products which features are not securely embedded to their products (Alba, 2015; Kitchin, 2014).

However, the theory by Kitchin & Dodge (2017) can be improved in various aspects. First of all, the theory can benefit from broadening the scope of smart city stakeholders. More specifically, it misses the involvement of citizens in the discussion of cybersecurity. The importance of citizens as a stakeholder of the smart city is recognized in smart city research. IBM describes this paradigm as "IN3": the paradigm of Instrumented, Interconnected, and Intelligent (Elmaghraby & Losavio, 2014, p. 492). At varying levels of smart city systems, citizens and smart city components are interconnected through various instruments, such as sensors and smartphones. This interconnection provides intelligent smart city services for the citizens. Meanwhile, data exchanged between the citizens and system generates feedback and advances machine learning, making smart city system more intelligent. Diverse data is involved in IN3, and the way data is being used within IN3 creates security and privacy concerns. The cybersecurity challenge in relation to citizens as a stakeholder is in line with the research by (Bekara, 2014). Elmaghraby (2014) points out that smart city technologies should aim to ensure widespread participation where

citizens are not only generating data but also mixing their personal knowledge and desires to the smart city design.

The second aspect the theory by Kitchin & Dodge (2017) can improve is to engage the discussion of privacy. Discussion of privacy concern is lacking here whereas it is considered significant in the research of Bekara (2014) and Jokar et al. (2016). Jokar (2016) discussed the ownership and accessibility issue of cloud-stored data. They suggested anonymization of the data to decrease the chance of data attribution to a particular user. Attention to privacy concern is also outlined in the research of Elmaghraby (2014). In this research, the importance of the connection between a smart city and its citizens when analyzing data security is stressed by the author. In order to realize the vision where the development of smart city takes place with a bottom-up approach, privacy and security are key risks and vulnerabilities that need to be addressed. Privacy concern is categorized as such: 1). "privacy" and confidentiality of the information 2). integrity and authenticity of the information and 3). the availability of the information for its use and services (Elmaghraby & Losavio, 2014, p. 493). The first category refers to the risk of data being read by an unauthorized person who is not the owner of the data. This risk is reflected by the cyber insecurity of eavesdropping by Bekara (2014). The second category is in line with the risk of impersonation/identity spoofing (Bekara, 2014) and identity theft (Depuru, Wang, & Devabhaktuni, 2011), where theft for electricity, health care and etc. may be committed through changing the user identity. The third category is stated as open data principle in (Janssen, Charalabidis, & Zuiderwijk, 2012; Kitchin, 2014a). It entails a principle of opening up data for wider reuse, and at the same time, providing accessible tools for analysis (Kitchin, 2014a, p. 2 of 17 Chapter 2). It means that open data does not limit to one focus of business or scientific purpose. It is data that is open to access, free to use and reuse, and a public and commercial value. Thus, open data mends the conventional division between public organizations, private companies and users (Janssen et al., 2012). As pointed out by Elmaghraby (2014), the risk of compromising the open data principle should be included in the analysis of privacy concerns. By discussing the stakeholder role of citizens and the privacy concern, Elmaghraby (2014) provided insight into the governance aspect of cybersecurity. Batty (2012) offered a more comprehensive analysis of smart city governance to counter cyber risk and vulnerability. To achieve so, Batty (2012) suggested governance, policymaking, and planning as three means.

2.2.2 Theoretical Framework

Based on the above literature review, this research builds the theoretical framework of smart city cyber risk and vulnerability in 2.2.1. This framework reflects the research focus of both technoogical and organizational aspects by 1). adopting the majority of the theory distilled by Kitchin & Dodge (2017) which covers all important technological dimensions of cyber risk and vulnerability and 2). including the organizational aspect of cybersecurity based on the research of Elmaghraby & Losavio (2014), Bekara (2014) and Jokar et al. (2016). Reason to adopt the theory by Kitchin & Dodge (2017) is that the theory covers most technological concerns of smart city cyber risk and vulnerability. It has done so without leaving out a certain smart city function or technology. It is shown in 2.2.1 that other research reflects the findings of Kitchin & Dodge (2017), making it a credible benchmark for cybersecurity analysis of smart city technologies. Yet, it is also discussed in 2.2.1 that wider consideration of smart city stakeholders and the governance aspect should be included in the spectrum of smart city cybersecurity. Therefore, additions of multi-stakeholder dynamic and privacy concerns will be made to construct the theoretical framework of smart city risk and vulnerability.

As result, seven dimensions of smart city cyber risk and vulnerability are constructed in this theoretical framework, which are:

I. weak software security and data encryption
II. system and maintenance insecurity
III. risks from the complex attack surface
IV. cascade effect of interrelated systems
V. human error
VI. multi-stakeholder dynamic
VII. privacy concern

The following section will demonstrate each dimension of the theoretical framework. Each dimension is summarized based on the literature review in 2.2.1.

I. Weak Software Security and Data Encryption

Cyber insecurity resulted from weak software and encryption is the risk and vulnerability that concerns every part of the smart city system. Smart city design needs to be aware of its structure in public organizations, as well as services and devices provided by private companies. It is not realistic to counter this risk and vulnerability solely through technological methods due to a large amount of coded embedded in the system (Batty et al., 2012). Thus, a combination of organizational and technical approaches should be applied aiming to reduce this consequences of this risk. It is important to build a mechanism of system testing before implementing any smart city projects. Attentions should be payed to the crucial stages before the smart system is fully implemented in order to find cybersecurity weakness and fix accordingly. Concerning the cyber insecurity of private partners, it is crucial to have the proper selection of private partners with pre-defined criteria. Selected private partners should comply with the cybersecurity standard put forward by the city.

II. system and maintenance insecurity

Two main concerns from this cyber insecurity are outdated software and legacy systems. Software applied in the smart city need a regular update to deal with emerging new risks and attacks. It is, thus, essential to have a cybersecurity team that manages the update and patching of the system. When newly developed software has to be implemented into existing systems, it is important to access the security of such implementation to avoid zero-day exploits.

III. risks from the complex attack surface

This risk comes with the intensive use of IoT devices in a smart city. The components such as sensors and meters that are spread across the city to gather data create a large surface for attacks. Thus, security measures to monitor and verify the data that are gathered through the components are necessary. Meanwhile, a mechanism to response to irregular signals timely should be built.

IV. cascade effect of interrelated systems

Interconnection of systems in smart city presents the risk of cascade effect. This risk needs to be considered when connecting a smart system to traditional systems and smart systems to each other. Vulnerability assessment should take place before the action of connecting these systems. It is crucial to consider the isolation between systems. In order to do so, smart city design should consider data can smoothly flow through systems without creating cascading risks.

V. human error

The human error refers to unintended mistakes and inappropriate handling of cyberattacks. It excludes the malicious intentions by attackers as listed in Kitchin & Dodge (2017). For the reason that the malicious attacks are conducted through exploiting other risks and vulnerabilities in this framework. In order to prevent the risk of human error, the staff of smart city projects should receive proper cybersecurity training. If a human error occurs, such as employee opening phishing emails, a cybersecurity team should be in place to mitigate further risk and damage.

VI. multi-stakeholder dynamic

Four smart city stakeholders which the risk and vulnerabilities attributed to are put forward to further understand the risk and vulnerabilities: (1) Technology Companies and Internet Service Providers, (2) Policy Makers, (3) Employees and users of the system, (4) Citizens. The multi-stakeholder dynamic of the smart city should be considered separately from other features of smart city, especially regarding cybersecurity. Even though, the multi-stakeholder model creates other cyber risks and vulnerabilities that are listed in this framework. It is worthwhile to explore a governance solution to this risk and vulnerability, rather than dealing with it only with technological solutions. It is crucial to have clearly defined and well-negotiated terms with service providers and data providers. These terms include, but are not limited to the clearly defined responsibility of fixing the cybersecurity issues (Kitchin & Dodge, 2017). For example, when a software service provided by the private company shows insecurity in its encryption, the private company should be responsible for patching and enhancing its security level.

VII. privacy concern

Main private concerns are 1). privacy and confidentiality of data 2). integrity and authenticity of the information and 3). open data. A smart city should consider the security measures to ensure that unauthorized access to personal data can be prevented and detected. Measures should be taken to verify and protect the identity of data owners. And the process of embracing open data principle should always bare the privacy and security concerns in mind.

A table of overview presents the seven dimensions of smart city cyber risk and vulnearbility theoretical framework and their relation to the research focus is shown in figure 1. Based on the

literature review and the primary theoretical framework, indicators will be operationalized to guide the case study. This operationalization will be detailed in 3.3.

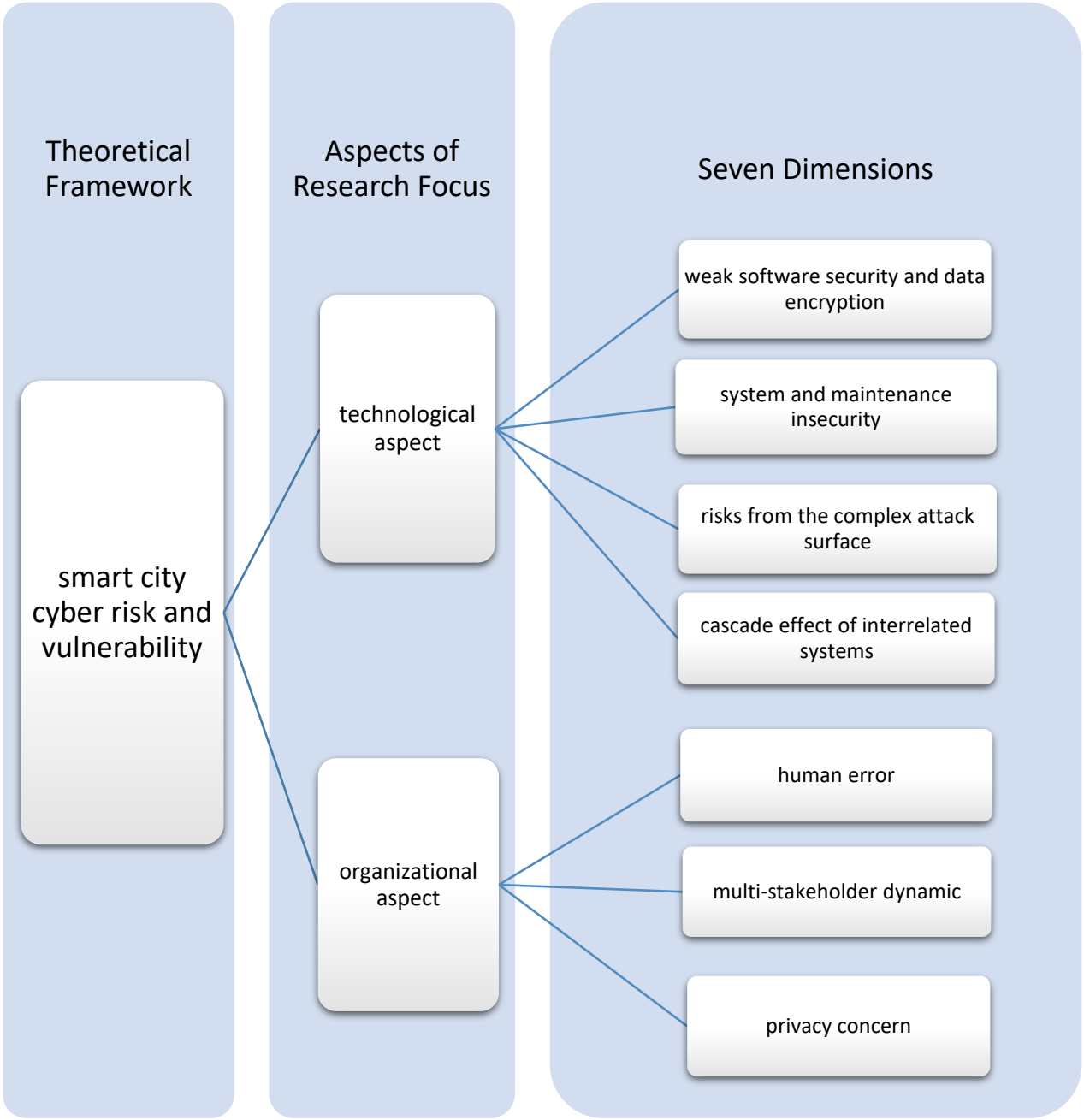

Figure 1. Theoretical Framework of smart city risk and vulnerability

Chapter 3 Methodology

3.1 Methodological Framework

3.1.1 Single Case Study Design

The case study is a research strategy that has a focus on understanding the dynamics of a phenomenon within single settings (Yin, 2003). The method of case study is valuable at all stages of the theory building process and commonly used to conduct various aims, including to provide a description, to test theory, or to generate theory (Bennett, 2004)). There are two motivations for choosing a case study design. In line with the guidelines provided by Yin (2003), case study assesses the form of the research question: whether the researcher possesses control of behavioral events and whether the research focuses on contemporary events. Research into cybersecurity policies is a study of contemporary and factual analysis instead of an experiment. The second motivation of case study design is due to the aim of this research. The main focus of this study is to test the theoretical framework of smart city cyber risk and vulnerabilities in order to contribute to the body of knowledge. It is especially relevant at the stage where candidate theories are "tested" (Bennett, 2004). It is argued by Eisenhardt (1989) that theories built from case study research are especially suitable for new topics which is applicable to smart city with open innovation characteristics. The result theory through this methodology is often novel, testable and empirically valid (Eisenhardt, 1989).

The means of case study is through a holistic in-depth single case study, focusing on one specific city context. It is a research approach that focuses holistically on a research subject under one context (Yin, 2003, p. 40). The method of a holistic in-depth single case study is chosen for two reasons. Introduced in Chapter 1, smart city with open innovation characters are rather new and under-researched, especially regarding cybersecurity. Open innovation is an increasingly influential new approach to smart city development which links technologies with the citizens, the urban territory and other cities (Paskaleva, 2011). Such a representative or typical case is one of the most common rationales for choosing a single case study design (Yin, 2003, p. 41). Another motive for choosing a single case study design is the encouragement of holistic approach in smart city research pointed out by past literature. Lombardi, Giordano, Farouh, and Yousef (2012) constructed a model for smart city assessment. The model emphases the measurement of a smart

city policy which should consider the holistic, interrelated and multi-stakeholder concept. It is important to adopt a specific and holistic approach by taking into account the regional features of the city context (Mattoni et al., 2015). It is crucial to have a holistic focus when conducting policy evaluation of a smart city, in order to fill the knowledge gap in an "often normative assessment" (Castelnovo et al., 2016). Bearing the above motives in mind, the holistic case study design is selected as for a case study design provides the opportunity to explore and understand a complex issue, especially when in-depth analysis is needed.

Additionally, logical subunits within the context of a smart city can be identified, being the smart city projects. Thus, it constitutes a single case study with embedded units of analysis. The research will carry on by assessing the cybersecurity policies of subunit projects and gather the research for an in-depth single case study. The aim of an embedded design is to increase the robustness of the holistic approach. By addressing different subunits of the research subject, embedded design can serve as an important device for focusing the case study inquiry to the central research question (Yin, 2003, p. 45).

3.1.2 Case Selection

This research has a scope of case selection of smart cities with a feature of open innovation. For the reason that it is a new phenomenon with limited research conducted in regard to cybersecurity. The Netherlands presents as a suitable research subject being a pioneer in open innovation and integrated urban development (Smith, 2018). Different from many government-led smart city projects, the Dutch smart city approach is bottom-up. Cities work towards their smart ambitions with local initiatives that are discussed with citizens and piloted together with companies (Mol, 2015). Citizens are no longer only receiving the result of smart city development, but also participating, shaping and building the smart city. Moreover, the foremost important goal of smart city technology is to establish a smart society that can continuously serve urban life (Switch, 2018). Another distinct feature of smart cities in the Netherlands is the innovation-driven approach with close collaboration with top universities. For example, Eindhoven focuses on six research lines with Eindhoven University of Technology (TU/e) on Smart Cities Programme (TU/e, 2018). Smart city strategy, on the other hand, shares the common features like a complex and interconnected

system enabled by IoT. All the above constitutes a perfect candidate for the research subject of open innovation.

Moreover, this research selected the City of Eindhoven as the research subject. It is due to its common features of open innovation as other Dutch smart cities, as well as the impact of Eindhoven smart city on other Dutch smart cities. These two reasons are explained in the following paragraphs.

The first reason is the open innovation characteristics of Eindhoven smart city projects. The municipality of Eindhoven is actively building a pioneering smart city with the qualities of technology, design, and knowledge (Gemeente Eindhoven, 2019). Eindhoven municipality has formed a Smart City Continuous Innovation Process (SCCIP), along with TU/e, Philips Lighting and their partner Heijmans. The process features the citizens of Eindhoven as a basis of smart city innovations, together with three other key stakeholders: the municipality itself, businesses and research institutions, furthering the smart city development (Brock, 2016). Eindhoven seeks to deliver real solutions to sustainability and smart living, creating the world's first "crowdsourced" smart city with open innovation mentality (Cities Today, 2016). The characteristics of open innovation in Eindhoven smart society initiative are manifested in various smart city projects.

As a participant of 'Lighthouse City' for the European Union's Horizon 2020 Triangulum project, Eindhoven is seeking to drive smart city innovations globally by demonstrating real solutions that are smart, sustainable, and inclusive (Triangulun, 2017). The district of Strijp-S is being transformed into a sustainable smart community from being a former Philips Industrial complex. The city is making use of the remediation process to generate energy while transforming the area into a creative smart district (Smith, 2018). The district also manages public safety by means of sensors detecting the sound of a window pane breaking or a chain lock clinging and warning nearby police (Brainport, 2016). Residents of the district will also be provided with the smart infrastructures such as shared electric cars service or using the smart parking space (Triangulun, 2017). Apart from smart living complexes, as the "city of light" (Interview on 28 June , 2019). Eindhoven is also focusing on innovative solutions to urban lighting. The focus of urban smart lighting is not only aiming at reducing the energy cost by adaptive lighting technologies but also to provide desired services based on the need of citizens. Alternatively, smart sensors in each LED luminaire may be utilized to adapt the lighting to weather conditions or provide light on demand

when people are on the streets at night to improve safety (Cities Today, 2016). Moreover, another outstanding example of crowdsourcing in Eindhoven is Stratumseind 2.0 project. Lampposts on the street Stratumseind are equipped with sound sensors and counting cameras to monitor the crowd behavior in order to realize functions such as alerting the police in case of a street fight (Dijk, 2018). The technology ecosystem Brainport smart district strives to be an innovation hub and a strong economic driver in the Netherlands (Smith, 2018). The district is constructing entirely new infrastructure to facilitate future innovations.

The second reason is the impact of Eindhoven smart city projects on the practice of other smart city projects. The experience of open innovation is valuable to other smart cities in the Netherlands. City of Eindhoven is the base of a start-up non-profit foundation The Dutch Institute for Technology, Safety & Security (DITSS). Founded by governmental and research organizations, DITSS has expertise in building smart innovation communities and platforms in ways of living labs. The experience of Eindhoven smart city projects is shared via DITSS. Meanwhile, the City of Eindhoven provides tools to accelerate the development of other smart cities. The policy instruments and technology of Eindhoven smart city can be downloaded through Smart City StarterK!t. Thus, it is reasonable to argue that choosing the City of Eindhoven as the research subject is theoretically justifiable and practically valuable.

To sum, the smart city projects are identified as subunits within the subject of smart city Eindhoven. Unit of analysis is the policies aiming to prevent and mitigate cyber risks and vulnerabilities of smart city projects in Eindhoven. A table displays the characteristics of smart city Eindhoven in Table 1.

Eindhoven smart city projects	
Service and Function Focuses	Crowd management Smart urban lighting Smart mobility Smart communication and interaction with citizens Sustainability and energy efficiency Safety
System Design Focuses	open innovation multi-stakeholder cooperation
Applied Technologies	Real-time sensor monitoring and AI analysis IoT sensors Big data
Aim	Achieving a smart society
Characteristics	privacy first open data and interfaces embrace open standards share where possible support modularity maintain security accept social responsibility
Projects involved in this research	Strijp-S Brainport Stratumseind 2.0 Project Smart lighting projects Smart Mobility Projects

Table 1. The Characteristics of Smart City Eindhoven

3.2 Data Collection and Sources

The six most commonly used sources of evidence in case studies are documentation, archival records, interviews, direct observations, participant-observation, and physical artifacts (Yin, 2003, p. 85). To strengthen the internal validity, unit of observation is triangulated by documents, interviews and direct observations. The method of documentation is chosen to conceptualize the case study that utilizes in the concept of smart city risk and vulnerability. Open source documents and reports of the smart city projects in Eindhoven offer an important understanding of the policy focus regarding the overall development of these projects. In line with the strategies put forward by Yin (2003), the research strategy of interview is chosen by assessing the form of the research question: whether the researcher possesses control of behavioral events (Yin, 2003, p. 88). The research topic focuses on contemporary developments and requires analysis to interview transcript instead of control of variables to the subject. Further, the research into cybersecurity policies applied in the booming development of the smart city projects calls for timely and urgent empirical research (Schneier, 2017a), which the open-source documents alone cannot provide. Therefore, the interview method is chosen appropriately to answer what are the policies developed against cyber risk and vulnerabilities. Additionally, while the interviews take place, some projects are visited for direct observation, to supplement the other two data collection methods. Triangulation is an important principle of data collection (Yin, 2003, p. 97). Using multiple sources of evidence is likely to strengthen the research by making it more convincing and accurate (Yin, 2003, p. 98).

Regarding the specific manner of caring out the interviews, semi-structured elite interviews are chosen to be conducted with security experts in Eindhoven smart city projects. Elite interview is preferred when attempting to address policy and enter a network of an industry (Gillham, 2005, p. 59). A semi-structured interview is a flexible and valuable way of obtaining qualitative data (Gillham, 2005, p. 70). It is best used when conducting small-scale research (Drever, 1995). The questions of the semi-structured interview are open with the opportunity of asking for additional questions with probes. This gives the chance to gather data on cybersecurity of Eindhoven smart city projects beyond the theoretical framework. The cybersecurity policies center around the specific security focus of involved projects and are limited to the scale of Eindhoven. Therefore, a semi-structured interview is the most suitable form of interview for this research. The same questions will be asked to all interviewees involved. Meanwhile, the interviewees are prompted

by supplementary questioned to ensure that all aspects of the questions are dealt with. In turn, semi-structured interviews provide the interviewer with some freedom to explore certain phenomena described by the interviewee and thus create more distinct data (Yin, 2003). The interview framework will be designed using the indicators from the theoretical framework where each question will be dedicated to address one dimension of cyber risk and vulnerability. The specific interview questions are presented in the interview framework in Appendix III. Interviews will be conducted in the smart city projects and initiatives in Eindhoven, which are Strijp-S, Brainport smart district, Stratumseind 2.0 Project, Smart Lighting Projects and Smart Mobility Projects. The confirmation bias will be reduced by briefly discussing the answers with the interviewees following the guidance of prompts.

3.3 Operationalization

3.3.1 Indicators

Despite the fact that there are many studies that have provided important information about the risk and vulnerabilities about specific smart city projects, there is no standardized set of cyber risk and vulnerability analytic indicators that can be applied to assess the current risk and vulnerability in upcoming smart cities (Watts, 2003). The literature above has identified various common cyber risk and vulnerabilities (Cerrudo, 2015; Kitchin & Dodge, 2017; Townsend, 2013). Based on the theoretical framework, the concept of risk and vulnerability will be distilled into indicators to be applied to the case study of Eindhoven smart city projects.

The purpose of deriving indicators is to help minimizing the difficulty to demonstrate the relationship between the abstract dimensions and patterns in risk and vulnerability analysis (Aven, 2007). In this case study, two reasons that indicators are demonstrated. That is, first, indicators will help to scrutinize the data collected as detailed as possible in order to avoid the tendency of simplifying and generalizing the cyber risk and vulnerabilities. The indicators also serve as tools to identify to which dimension of cyber risk and vulnerability the data is related to. That was the second reason for using indicators.

Based on the theoretical framework, every indicator presents its own signals to be identified. (1) A large amount of code that contains potential zero-day exploits includes programming bugs.

Much to this indicator of risk is unable to be detected nor prevented, thus, the analysis to this risk is difficult to carry out. The measures to counter this risk would be to minimize the potential of this risk through system testing before an operation. For instance, hacker teams can be brought in to try to test whether there is programming bug so that the technicians can still take actions to fix them. (2) No or minimal security for the system. It refers to the vulnerability of the system generated due to poor awareness of the potential attacks, for example, using default or simple usernames and passwords. The assessment of this vulnerability can be achieved through identifying policies regarding cybersecurity training for the employees and the users of the system. Such training including the awareness of the forms of attacks, the proper way to safely interact with the system, etc. The policies to prevent this risk can also present at mandatory and regular password changes and system updates. (3) Technologies that are not tested for cyber resilience is alarming when technology is put to operation without proper testing. Different from the first risk signal, this indicator is particularly relevant for technologies and services provided by partners of the smart city projects, such as the provision of smart lighting installations from Philips in the Jouw Licht Op 040 project. The signal to identify this risk lies with the actions taken by the project from the very beginning of the cooperation. For instance, the negotiation of which party has what right to data management at the beginning of the partnership. (4) Unmonitored end-to-end security in IoT applications is caused by various sensors and low-powered devices on an IoT system that cannot fully support the encryption of more complexed system (Cerrudo, 2015). The components of IoT are made smart to be controllable from a distance and to generate information about their use. Such signals can be identified through the measures taken against lacking encryption in the IoT components, for example, cameras and lights. (5) Poor security on legacy systems creates forever-day exploits that are proven to be difficult to test, therefore leaves inherent cyber vulnerabilities (Cerrudo, 2015). The effective way to prevent legacy system issues is to build new infrastructure that complies to the security requirements of new technolgy. (6) Poor security isolation among interconnected systems can compromise the individual systems even when they are by themselves secured, additionally creates the possibility for the cyber risk to spread from lower-powered, less-critical system to higher-powered critical system (Townsend, 2013). Policies regarding the security of network traffic and data up/downloading routes can indicate how this risk is being prevented. (7) Human factor includes accidents that are innocent yet maybe due to lack of security training, and malfeasance of insider or outsider’s compromises (Cerrudo, 2015). Human

error can be significantly exploited by cyberattacks in ways of phishing emails, viruses or malware. Training on cybersecurity or an adequate cybersecurity management team are crucial in preventing this type of risks. (8) Cybersecurity arises from the complexity of multi-stakeholder dynamic. Public-private partnership is often applied in smart city design. It is important to ensure the responsibility of each partner facing cybersecurity challenges. The selection of properly secured partners is necessary to reduce cyber insecurity. Furthermore, the security concerns of linking systems of public and private organizations need to be taken into consideration. Secure routes of data flow in data management are crucial to prevent risks of multi-stakeholder dynamic. (9) Privacy of users should be addressed on organizational level as well as on technological level.

3.3.2 Operationalization Scheme

The table of the operational scheme below displays the indicators relevant to the dimensions of risk and vulnerability in the theoretical framework. Furthermore, more extended signals to identify and assess the indicators are provided in table 2. This table is primarily created based on the theoretical framework and will be extended through data collection and analysis.

3.4 Analysis Scheme

Bearing the outlined indicators in mind, interviews and available documents are systematically analyzed of smart city cyber risks and to demonstrate, the assessment goes through the following questions:

- What factors of risk and vulnerability (indicators) are presented during the case study?
    - Which dimension of the cyber risk and vulnerability do the factors indicate?
    - To which stakeholder does the factor attribute to?
- What are the main concerns of cyber risk and vulnerability according to the interviewees?
    - To which stakeholder do the risk and vulnerability attribute to?
- What cybersecurity policies are applied to prevent and mitigate the cyber risk and vulnerability identified?
    - How do they contribute to the theoretical framework of smart city cybersecurity?

	operationalization scheme								
Indicators	Large amount of code that contain potential zero-day exploits	No or minimal security for system	Technologies that are not tested for cyber resilience	Unmonitored end-to-end security in IoT applications	Poor security on legacy systems (forever-day exploits)	Poor security isolation among interconnected systems	Human factor	Public and private partnership	Privacy of users
Dimensions	Software Security and Data encryption Human Error	Software Security and Data encryption Human Error	Software Security and Data encryption	Software Security and Data encryption Large Attack Surfaces	system and maintenance insecurity	Cascade Effects Large Attack Surfaces	risks from the complex attack surface Human Error	system and maintenance insecurity cascade effects of interrelated systems risks from multi-stakeholder	privacy concern
Signals (example)	hacker tops; system testing period before operation; living labs; check whether the partners test the security of their service/product before providing them to the smart city	Security training; third-party credentials	Security checks on the partners; Data ownership; automation of the partners; weak authentication; the inherent trust of the systems from the partners (vendor backend APIs)	Security assessment towards the applications such as sensors and cameras; encryption on IoT components	the upgrade of old operational devices; security checks to legacy systems	Security checks on the routes of data in IoTs; security on network traffic	Recruitment and preservation of cybersecurity talents; Appropriate security software; security training on identifying phishing mails and avoiding viruses or malware	Public-private partnership; Predefined terms and responsibilities in partnership; Data exchange; Trust of partners' security standard; verification of partner's data	Privacy law requirements; application of open principle; data ownership; personal data
stakeholder	❖ Technology Companies and Internet Service Providers ❖ Policy Makers ❖ Employees and users of the system ❖ Citizens								

Table 2. operationalization scheme

3.5 Limitations

The first aspect of limitation of this research is accompanied by the data collection methods. For each smart city project, elite interviews are conducted. From which, snowballing will make it possible to reach more interviews. Such a method is possible to be a subject of politically acute and controlling, as well as influenced by hidden agendas that might underpin the interview (Gillham, 2005, p. 59). The limitation is posed by the bias and concealed answers given by the interviewees. Due to the need to rely on the interview method, there can be potential vulnerability or risk that the project (team member) does not want to share. In order to limit the negative effect of this method, this research strives to include interviewees from various department of the smart city project, such as project developers, field operators/users, technology providers, and relevant research facilities. Interviewees might project their agenda or bias to the answers they give. Thus, this research tries to identify true information with the aid of detailed indicators. This research will bear this in mind and try to ensure the objectivity by offering confidentiality and compare the answers to published reports.

The availability of documentation for analysis can also be a limitation. A lack of publicly available information regarding the policymaking for a specific project may mean that some less reported or influential projects are excluded from this study. The "selection effect" (Berk, 1983) might be connected to the characteristics and the publicity of the projects in the manner that the most mature and reported projects are likely to be represented more in this research. Therefore, cases selected are a reflection of the main characteristics of the smart city Eindhoven development. For instance, cases that are closely associated to open innovation. Additionally, a triangulated method of data collection will strengthen the validation of the data by supplementing and validating the data produced by one of the sources.

Another aspect of limitation comes from the design of a single case study. This research design refrained from gathering data from more smart cities due to the preference of a holistic in-depth case study from smart city literature. It is also due to feasibility concerns. It is possible that specific technology or circumstances cause smart city projects to present or conceal certain vulnerabilities and risks. The characteristics of open innovation are important in shaping the smart city policies

in Eindhoven, which does not necessarily apply to other smart city projects. Therefore, drawing broader conclusions is not aimed at in this research.

Chapter 4 Analysis

This chapter will analyze the data collected from Eindhoven smart city projects, applying the theoretical framework constructed in 2.2.2. The interviews used in this analysis were conducted with experts from Stratumseind 2.0 project, municipality of Eindhoven, smart mobility, smart lighting and Brainport smart district. The first part of the analysis will test each dimension of the theoretical framework. The second part of this chapter will be the analysis of measures presented during data collection that are beyond the theoretical framework.

4.1 Testing Theoretical Framework

The city of Eindhoven brings attention to the serious impact of the collected data and the intensive implementation of IoT technologies on urban life. Common principles are put forward by the City of Eindhoven that are applied to smart city initiatives in the city. The principles entail the characteristics of Eindhoven smart city projects, which are: privacy first, open data and interfaces, embrace open standards, share where possible, support modularity, maintain security, and accept social responsibility (StarterK!t, 2015b; Triangulun, 2017). The principles encompass the cybersecurity measures taken by the projects and focus the security effort on openness and privacy. Guided by the theoretical framework, this chapter will outline the cybersecurity concerns in Eindhoven smart city projects and analyze the cybersecurity policies and measures the projects apply. The municipality of Eindhoven is leading the development of various smart city projects in the city and has a structured cybersecurity mechanism. Meanwhile, each project has its own cybersecurity focus and measures. This analysis will look into the cybersecurity measures, taking the roles of the projects and the municipality into account.

I. weak software security and data encryption

It is inevitable that software coding and encryption cannot be perfect and bullet-proof. In alliance with the theoretical framework, two effective approaches to prevent errors to compromise the operationality of the smart city projects are identified: technical and organizational approaches.

The technical approach is to develop testing mechanisms consisted of testing period and an ethic hacker team. Eindhoven smart city projects all go through a considerable testing period before going into operation. Eindhoven smart city projects adopt a living lab model which enables the projects to be tested and learned from while providing services to the citizens. In fact, some projects are still under testing as living labs since a few years. For instance, the Brainport smart district is still in early stage of constructing a living lab, testing the development of an innovation hub (Interview on 27 June, 2019). Living lab itself is a measure to prevent the errors from the software design and encryption causing negative consequences to the smart city systems due to the giving testing period before wide implementation. It is notable that the smart lighting projects have a different model for testing in this respect. The pilot projects of Jouw Licht Op 040 started with the process of building infrastructure which is implemented into the daily use of citizens in long-term. Yet, with a closer inspection, it is clear that Jouw Licht Op 040 project takes testing period for operationalizing the smart technologies that would be applied to the infrastructure (Interview on 28 June, 2019). Therefore, there is no exception that Eindhoven smart city projects all adopt testing period in forms of living lab or pilot for ensuring the cybersecurity of the projects. Living lab as a measure for cybersecurity will be further elaborated in the section Living lab: learning by doing. The testing is regularly maintained by a team in the municipality. A team of ethic hackers are engaged in the process of testing. Every year, the managing team in the municipality has a meeting with the ethic hackers regarding the details of safekeeping the smart city projects. The ethic hacker team that assists Eindhoven to achieve its cyber secured smart society is consist of experts in the region. They have a very connected community in which the hackers communicate with each other about new discoveries of security breaches. Thus, the size of this ethic hacker team is described by Interviewee 2 as “bigger than what I could imagine” (Interview on 21 May, 2019). This team of ethic hackers is an important measure to mitigate the potential zero-day exploits in the system design before going operational.

Organizationally, the municipality puts its focus on the way they cooperate with third parties when trying to minimize the risk from weak software security and data encryption. When cooperating with third parties, the smart city projects do not inherently trust the security level and standard from the partners. Before signing the contract, there are negotiations, checks and tests on the company’s security standards. Of which, security standards are cross-checked on both sides: the

municipality and the companies. According to the municipality of Eindhoven, codes are cross-checked among partners before putting to use.

However, each project engages these two approaches in different levels, of which two projects present vulnerability to zero-day exploits. The floating car data project of smart mobility, for example, does have a five-year testing period but does not engage a hacker team to run tests (Interview on 5 June, 2019). The traffic management team is aware that more resilient mechanism must be developed to manage the cybersecurity of partners once the project goes into wider implementation. Similarly, no pre-testing measures such as hacking tops are employed in the implementation of smart lighting projects. But it was commented by Interviewee 5 that it is important to set up such mechanism for implementation on a larger scale (Interview on 28 June, 2019). From the comments on the ethic hacker team measure, it is clear that the smart lighting and smart mobility projects are aware of the zero-day exploit risk and the necessity to employ testing team. However, the implementation in this respect is lacking in these two projects.

Additional measures to ensure software security is made by the municipality together with the smart city projects. For instance, the municipality of Eindhoven is making the effort to set application program interface (API) agreements for private partners to comply with. This effort is being supported by smart lighting and the Stratumseind 2.0 project (Interview on 28 June, 2019; DITSS, 2017), based on the Future Internet Middleware for Smart Cities (FIWARE). FIWARE is an architecture proposed by EU in safeguarding the smart city projects (Mol, 2015). Eindhoven projects adopt FIWARE to enhance the accountability due to its requirements of visibility in every layer of the system (Interview on 22 October , 2018). These technical measures are part of European effort to ensure smart city cybersecurity, providing architectural support.

The risk of weak software security and data encryption is a serious concern of the smart city projects in Eindhoven and the municipality. The cybersecurity policy against this risk and vulnerability dimension can be categorized as technical approaches of setting up ethic hacker teams and using testing period and organizational approaches of checking and testing the partners in the contract phase. Ethic hacker team is not yet being employed by the smart city projects except for the municipality who oversees the projects. The measure of testing period is, on the other hand, applied by every project. Most of the projects rely on tests and checks on the security level of partners in the contract phase to ensure software and encryption security.

II. system and maintenance insecurity

The most concerning system and maintenance insecurity in a smart city project is the issue of legacy system. On one hand, transforming traditional urban functions into smart interconnected systems requires layering new technologies on old infrastructure. The best way to avoid being undermined by legacy systems is to completely rebuild and replace the infrastructure. However, some basic infrastructure such as the roads and energy grids require years of work to replace. On the other hand, even if possible, it is expensive to upgrade all the systems or simply replace the infrastructure such as lightings. Therefore, policy making needs to address what is the imminent upgrade that is the most necessary to spend the budget on. Legacy system is an issue recognized by the municipality of Eindhoven in its smart city projects. At this stage, living labs are the main focus of smart city projects in Eindhoven. Therefore, the infrastructure most relevant to the purpose of the projects are the priority to update. It is the intention of attracting more investment and ministry funding by showcasing the success of living labs (Interview on 5 June, 2019).

The smart lighting projects face this challenge with building long-lasting infrastructure and continuous innovation. The smart light project focuses on the transformation of traditional lights into connected lights through IoTs. Among the infrastructure, the light poles and cables are traditional infrastructure that is being managed by the municipality which the smart lighting projects still make use of. The lights are upgraded which new software can be layered onto. These intelligent lighting units are not just vessels for the pilot projects, but also "long-term infrastructure that would be permanent as long as they can still provide the functions needed" (Interview on 28 June, 2019). Continuous innovation is the core to this solution. The result is that the lights will stay to host the innovation according to the needs of the citizens. In this way, the cyber vulnerability of legacy systems is avoided.

A similar approach is adopted by the smart mobility project of intelligent traffic management. Aiming to advance the traffic management system, the smart mobility team of Municipality of Eindhoven and Rijkswaterstaat[2] have been running an innovation experiment for five years. This pilot system runs on new infrastructure built on the side of the highway, called floating car data.

[2] Rijkswaterstaat is Dutch national department of public works and water management. It is part of the Dutch Ministry of Infrastructure and Water Management and responsible for the design, construction, management and maintenance of the main infrastructure facilities in the Netherlands.

The current traffic detection from Rijkswaterstaat is a classic system that has been running more than 25 years. It is custom-made for Rijkswaterstaat and functions well. However, it is not possible to layer newly developed software on this traditional system. In order to implement the floating car data, new infrastructures called “intelligent roadside units” (Interview on 5 June, 2019) will be built. With these units, Rijkswaterstaat will be able to add any new software processing data from private companies to the hardware of Rijkswaterstaat. Another part of the smart mobility projects also opted for an upgrade of the traffic lights. The previous dialing system which was vulnerable to hacking has been upgraded to the current digital system.

While requiring more time to achieve, the Brainport smart district also intends to build new infrastructure. The infrastructure is under construction within the smart district. However, it is not to be expected in the connected public area outside of the district, for example, electricity, train, etc. “We need to have money to run the project first”, as the initiator of Brainport smart district put it, the project needs time to attract investment by doing and showing what the project can achieve (Interview on 27 June, 2019).

From the data above, it can be concluded that due to the demand of upgrading the infrastructure, the risk of forever-day exploits in legacy systems is prevented in smart lighting, smart mobility and Brianport smart district projects. Although it is obvious that constructing new infrastructure for intelligent systems avoids the vulnerability of legacy system, this approach demands time and finance to carry out.

III. risks from the complex attack surface

End-to-end security is recognized as a serious concern by the municipality when linking smart systems to the original functions. This type of connection creates “extra points for intrusion” (Interview on 4 July, 2019). To manage the complex attack surface in a smart city project, it is important to address the vulnerability of interconnected IoT sensors. End-to-end security is thus crucial to be maintained by private partners and by the municipality. The municipality of Eindhoven does not manage end-to-end security for every project, such as smart lighting projects, because they are still on the contract phase (Interview on 28 June, 2019). It is, therefore, too early to provide analysis on end-to-end security in this phase of the project. However, future cooperation

on this subject is expected according to Interviewee 2, “it is not all very clear for every project” (Interview on 21 May, 2019). In Brainport smart city project for instance, it is not yet determined who is responsible for managing the risks from the IoT enables devices (Interview on 27 June, 2019).

Various projects look further than end-to-end security when assessing the risks from the complex attack surface. The Strijp-S project summarizes the attack surface in layers: the 'cloud layer' houses all data and online traffic. Analysis, communication and content development all take place in this layer. Next is the 'livable layer': the tangible part of the city. The streets we walk in and the doorknobs in our hands. Finally, there is the 'infrastructure layer': roads, railways, pipes and cables. The interaction between these layers makes the city smart. The layers communicate with each other and work together, thus creating crossovers and integrations. The interaction among the layers creates the cybersecurity risks by facilitating a complex attack surface. The smart mobility projects are most concerned with cybersecurity risk and vulnerability on the ‘cloud layer’ and ‘infrastructure layer’, namely, end-to-end security and cloud-based data security. According to Interviewee 3, advisor and coordinator active traffic management at Rijkswaterstaat, the partners manage the end-to-end security of IoTs, which is an agreement written in the contracts (Interview on 5 June, 2019). Same choice is presented in the smart mobility projects managed by municipality of Eindhoven. The partners are responsible for managing the IoTs and the municipality provides supervision and cybersecurity response with a team dedicated to smart mobility projects (Interview on 4 July, 2019).

The results of the interviews indicate that the risks from complex attack surface are mainly managed by relying on the cybersecurity management of the IoTs technology and service providers. On one hand, this approach optimizes the human resource in the municipality and the smart city projects for innovation and policy making. On the other hand, the trust on the private partners needs to be better understood and discussed. It was presented in the conversations with Interviewee 4 and Interviewee 5 that it is not an obvious understanding for the private partners to maintain end-to-end security in the Brainport smart district and smart lighting projects.

IV. Cascade effect of interrelated systems

The isolation among the systems includes the isolation between the projects and the municipality; between the private and public partners; and between the intelligent infrastructure and the traditional infrastructure.

Regarding the isolation among the projects and the municipality, they are managed separately, which leaves the projects responsible for cybersecurity on a daily basis. If a project's cybersecurity is severely breached, the municipality can choose to close that project down (Interview on 21 May, 2019). The municipality also prevents cascade effect with a system architecture that isolates the data platforms. The data platforms of each partner are managed separately but with same security standards so that they data can be combined through the platforms. In case of a hacking attack on one data platform, the other data platforms can cross-check and "they cannot come through to the other platforms" (Interview on 21 May, 2019). Therefore, cascade effect is not concerned by the municipality in safeguarding the traditional functions of the municipality.

Regarding the cascade effect from private partners, the projects prevent in different manners. In the floating car data project, the systems are not implemented outside of the pilot area at this moment. In case of cyberattacks on one private partner, the unusual data will be identified through comparing the data with other partners (Interview on 5 June, 2019). However, the cross-checking is the only feasible mechanism at this moment, and it is not sufficient for broader implementation in the future. It was pointed out in the interview that new algorithm needs to be developed in the future countering the cybersecurity risks from the private partners.

Regarding the cascade effect between the intelligent infrastructure and the traditional infrastructure, it is not considered to be very threatening since the management of these interconnected systems are rather separated. Smart mobility systems mostly stand-alone, posing very low risk to cascade effect. Unless the attacker has "a high-level access to the systems of the municipality", then it is impossible to carry out such attacks (Interview on 4 July, 2019). Otherwise, it is not really considered an issue in the domain of smart mobility. The Strijp-S also provided an example of managing the isolation between the intelligent and the traditional infrastructure. The intelligent cameras are placed in the light poles which are pre-existing city infrastructure. Attempts were made by attackers to physically access the sensors by opening the panel on the light poles with a screwdriver (Presentation by Strijp-S, 2019). The Strijp-S deals with this issue by setting alarm in the light poles so that they would send accurate location of the breach immediately for intervention.

According to Interviewee 4, due to the fact that Brainport smart district is not yet connected to the infrastructure outside of the district, cascade effect is not one of the cyber insecurities (Interview on 27 June, 2019).

The cybersecurity from cascade effect is managed by the smart city projects, yet, it is important to note that there are two folds of this conclusion. It may not be heavily concerned that a cyberattack on an IoT sensor might breach the citizens' data stored in municipality, but the data flowing through these systems are interconnected which could be manipulated (Interview on 4 July, 2019). This is possible by feeding the system false data deliberately since a smart city system produces information based on the data gathered through sensors in public spaces. Similarly, it is possible to manipulate the data of crowd management in the Stratumseind 2.0 project, by feeding the camera or sound sensors misleading information (Interview on 22 October , 2018). Thus, the data quality is more concerning in the respect of cascade effect than system compromise.

V. human error

The effective way to reduce the possibility of human error such as clicking on the phishing mails is providing cybersecurity trainings to the employees. This measure is not applied thoroughly in municipality of Eindhoven. According to Interviewee 2, employees do not work exclusively for smart projects or traditional functions within the municipality. What they work on depends on their specialization and preferred career focus. Training for all employees regarding cybersecurity are provided, however, are not mandatory (Interview on 21 May, 2019). Employees are thus, not necessarily aware of the threats of the cyber risk and vulnerability or the proper ways to react to threats.

The result of voluntary cybersecurity training is that a dedicated cybersecurity team is necessary to mitigate the risk of human error. Such a team should be in position to timely detect and limit the damage resulted in careless actions. The municipality has a team of cybersecurity for general operations of the traditional functions and all smart city projects, including the smart mobility, smart lighting, the Stratumseind living lab and Strijp-S, etc. (Interview on 4 July, 2019). They can, for example, effectively detect the phishing mails by screening the senders with a blacklist. Threats usually are detected before the employees have the chance to get in contact with the emails sent

from blacklisted senders. If odd emails reach the inbox of employees, they are encouraged to immediately ask for assistance of the cybersecurity team. Despite the effort of setting up a cybersecurity team in the municipality, it is undeniable that managing various smart city projects across the city on top of maintaining the traditional functionality of the municipality demands considerable amount of human power. It is suggested in previous research that CIO or CERTs in each smart city project is optimal. On one hand, the projects rarely have a CIO or a CERT dedicated to managing cybersecurity against cyberattacks. There is also no fixed cybersecurity team for each smart city project which poses higher risk of human error. On the other hand, the municipality does have a CIO and a chief cybersecurity officer. Meanwhile, the municipality ensures that there is one data protection officer for each smart city domain (Interview on 4 July, 2019). The team of data management is responsible for connecting the smart city projects and the execution of data protection. For example, five experts of the data management are managing Smart Mobility projects, of which some personnel is also involved with other smart city projects (Interview on 4 July, 2019).

It can be concluded that the risk of human error is given less attention when addressing cybersecurity in the projects. The lack of compulsory trainings and the lack of a cybersecurity team dedicated to each project can lead to high risks of human error. In this aspect, the municipality does contribute more attention to its cybersecurity team which can effectively detect threats like phishing mails. However, trainings to employees who have access to smart city projects are not mandatory.

VI. multi-stakeholder dynamic

The quadruple helix is a structure in which four stakeholders working as partners in the development of smart society Eindhoven. The four stakeholders are public organizations (e.g. governments), private organizations (e.g. internet service providers), knowledge institutes (e.g. universities) and citizens. It is a cooperation and integration of all partners and it is important to address the cybersecurity from a multi-stakeholder perspective. Not all projects are involved with all partners from the quadruple helix. With the example of the smart mobility projects, four types of stakeholders are recognized as Rijkswaterstaat and the municipality, private companies, service providers and technology universities.

First, among the public organization partners, the municipality of Eindhoven has the leading role. The municipality has the responsibility to approve and support the projects, as well as the power to pull the plug if deemed necessary. The involvement of Eindhoven smart city in each project varies. In smart lighting projects where the municipality is the main initiator, everything has to be approved by the city. Compared to Strijp-S which is led by private companies, the municipality is not involved in its cybersecurity management on a daily basis.

Public partners that help to improve the cybersecurity in smart city projects are not limited to municipality level. Public partners of smart mobility projects on a national level are Rijkswaterstaat and National Data Warehouse (NDW) (Interview on 5 June, 2019). They both share applications that can be applied to the smart mobility projects and both are involved in managing the cybersecurity in smart traffic management. However, it is difficult to implement the cybersecurityprinciples proposed by Eindhoven to Rijkswaterstaat, for the reason that they only comply to national regulations (Interview with Niels, 2019).

Dutch municipalities have committed to comply with the Dutch municipalities Information Security Baseline (BIG) since 2017, which is a cybersecurity partner on national level. The Information Security Service for Municipalities (IBD), which is the municipal counterpart of the National Cybersecurity Center (NCSC), responded to this and developed the Baseline Information Security Municipalities (BIG). The BIG is a self-regulation tool and consists of a set of security measures, including physical security, with which municipalities can achieve a basic security level in a fairly simple manner. Meanwhile, the BIG is a derivative of the international information security standard ISO27001, as a central standard with several specific guidelines, in this case for certain municipal situations. BIG consists of three parts: a strategic and a tactical baseline for different departments or functions within a municipality and a group of operational products. On one hand, many municipalities have IT security issues but lack the scale and budget to deal with this subject intensively. This way, the BIG provides guidance. On the other hand, the BIG clearly indicates the way in which information security can be arranged, which applies more and more regulation power on the municipalities. An additional advantage is that the BIG also sets several requirements for the purchase of products and services and the selection of a data center, for example, for a cloud environment. The municipality of Eindhoven falls under the regulation of BIG. Annual inspections of cybersecurity are conducted by BIG of which any security concerns

need to be addressed by the municipality. Otherwise, a very expensive fine would be issued to the municipality.

Second and the most discussed stakeholder is the private partner. Various projects demonstrate the way private partners influence 1). the data security 2). the cybersecurity in the technologies provided and 3). the cybersecurity in the process of cooperation.

An important trend of using smart technologies for traffic management is to engage multi-stakeholder partnership, especially with private companies. Rijkswaterstaat is trying to transfer from fully relying on their own system for data gathering to largely using data from private companies. This is mainly motivated by economic concern. Having private companies gathering data for the smart mobility projects can reduce the cost of employing road inspectors. There are two to three private partners participating in the pilot project for real-time traffic management. As data gatherers, the cybersecurity of the partners has a large impact on the quality of data. This is a serious concern for Rijkswaterstaat and the municipality. Data from the third parties are tested and used to implement in the new traffic management system (Interview on 5 June, 2019). According to Interviewee 3, in the pilot project of floating car data, the data from the cooperation with the private company flows in one direction: from private companies to the public partners. Therefore, there is no risk of compromising the data gathered in Rijkswaterstaat's traditional system. However, another smart traffic management pilot, talking traffic will engage traffic data flow in two directions: public to private and private to public. The mechanism to ensure the process of data flow can be securely executed is through cooperation with NDW (Interview on 5 June, 2019). Additionally, the data is always verified by Rijkswaterstaat's own traffic management system. It was pointed out by Interviewee 3 that once this partnership goes into the stage of full implementation, Rijkswaterstaat will largely reduce the data they collect to achieve optimal economic benefit. It is unknown at this moment how efficient would the verification of private partners take place in real-time traffic situation.

The private partners often serve as technology and service provider, which is the most pronounced aspect of the multi-stakeholder dynamic. For example, the Sorama in the Stratumseind 2.0 project. "The sound cameras – from the Eindhoven startup Sorama – are now so advanced that they know the difference between a gunshot, fireworks and breaking glass", says Interviewee 1, ensuring the cybersecurity when applying technologies provided by private partners is crucial to the success of

the projects. Apart from the 3D sound system by Sorama, sensors and cutting-edge camera technology by Vinotion is also crucial to the success of the Stratumseind 2.0 project (Atos, 2015). The projects are mainly relying on the cybersecurity efforts of the private partners. In smart lighting projects, Philips and Heijmans are responsible for developing the APIs for applications which are open for everyone. They are also responsible of addressing the security concerns of this project. Similarly, in smart mobility projects, the private partners are trusted to have a high cybersecurity standard due to the careful selection process for the partnership. This selection process is thus important factor to the cybersecurity of the projects.

This process of partner selection is handled with distraction and considerations of cybersecurity, as presented in the interviews. The process sometimes takes years to complete. In order to address the societal problems and the needs of the citizens, a public-private partnership is applied to the process of realizing the smart lighting vision of Eindhoven. Smart lighting initiatives in Eindhoven did not engage all partners at once. From 2013 on, dialogues with the market and private companies began to emerge. This conversation and negotiation of contracts continued till 2016 when the first contract period started (den Ouden, 2012). In this initiative, five consortia went through the selection process of three years and Philips and Heijmans eventually landed as the main partners of this project (Interview on 28 June, 2019). The aim is to build commercially available public lighting with interactive systems that is also customized to the needs of residents. One example would be one of pilot projects Jouw Licht Op 040. The goal of the project was to create social lighting by projecting interactive lighting information in an apartment building (Interview on 28 June, 2019).

Designing this system requires identifying the needs of the residents and researching the feasibility and risks. The research facilities such as TU/e are deeply engaged partners in this cooperation. The university checks and evaluates the smart lighting projects based on the needs of the solutions that the projects are designed to provide. Then based on the research and feedback of the citizens, the projects make open calls for innovation and service provision. Together with the residents, the projects implement the innovation to the smart systems.

The quadruple helix model is a revolution to the traditional contractual relationship between the private and public organizations. In a traditional contractual relationship, the private partners deliver goods or services to gain benefits and financial compensation from the government. The

government pays for the private innovation that they cannot develop on their own in order to improve the life quality of the citizens. The private partners are usually not fully involved in the dialogues of the system design (Villani, Greco, & Phillips, 2017). Contrarily, in this quadruple helix, the public and the private partners both bring insights to the projects every step of the way. This is enabled by continuous communication and information sharing. Unlike a traditional public-private partnership where the government contract services to contractors and buys products from the providers where the private partners have no influence on the projects themselves. Not only quadruple helix manages to achieve increased societal benefits through cooperation with the private partners whose aim is to increase their economic growth, but also enables this cooperation the possibility of continuous innovation.

The public-private partnership in the Stratumseind 2.0 project is a good demonstration of this quadruple helix model. The Stratumseind 2.0 project operates with a cooperation network with the City Pulse pilot, Synchronicity and the quadruple helix consisted of the municipality, Atos, Philips, TU/E, TU/T and the citizens (Atos, 2015). The municipality of Eindhoven is responsible for the administration and policy making of the Stratumseind living lab. Meanwhile, municipality of Eindhoven is the coordinator of the projects and partners. Philips and Atos are the main private partners for the living lab. Atos mainly provides real-time analysis of the data. Philips is the supplier for the smart lighting sensors. Eindhoven University of Technology and University of Tilburg are partnering with the Stratumseind 2.0 project to examine the design of the systems in terms of technology implementation as well as privacy standards.

To conclude, the smart city projects in Eindhoven mange the risk of multi-stake holder with a quadruple helix model. By engaging dialogues with the citizens, universities and private companies, the smart city projects ensure to incorporate the expertise in strategic policymaking and technological solutions. The Stratumseind 2.0 project is a positive example of the quadruple helix serving as an approach to prevent and mitigate cyber risk and vulnerability. Yet, it is important to understand that the quadruple helix model generates security concerns as well. The partnership with the police in the Stratumseind 2.0 project for example, requires a solid structure of privacy policies to deal with the sensitivity of personal information. It is concerned whether the desired information, such as facial image and geographic information can be provided to the police

without compromising its confidentiality to the private partners. The next section will investigate the solutions put forward by Eindhoven smart city projects in this regard.

VII. privacy concern

Eindhoven aims to achieve a smart society which safeguards the privacy of the citizens which is explained as more than the compliance with the General Data Protection Regulation (GDPR). The interviewees all stress the cybersecurity concern of privacy for a trustworthy public image. According to Interviewee 4, it is the belief of Eindhoven smart initiatives that the citizens must know that they are in charge of the data. “The ones that create the data must benefit from the data they produce and share” (Interview on 27 June, 2019), in ways of financial benefits or improved life quality. Some companies want to oversee the data they gather, which is most of the cases at this moment (Interview on 22 October , 2018). But that is what municipality of Eindhoven trying to change. This is entailed as the open data principle as a policy instrument put forward by Eindhoven (Ollongren, 2017; StarterK!t, 2015a). The municipality of Eindhoven justifies the collection of data such as noise level and counting of the visitors for specified goals (Gerwen 2013). The requirements that the private partners have to comply with is clearly defined in the Stratumseind 2.0 project. The requirements include but not limited to the (types of) technologies to apply, "how it would be explored and the specific functionalities as public utility" (Interview on 22 October, 2018). Partial data gathered in the smart city projects are already processed and present on the website of Eindhoven municipality[3], such as demographic data of smart mobility projects.

It is challenging to implement open data standard when the successful system relies on multiple stakeholders. This issue is being dealt with on multiple levels. Nationally, there are round-table discussions involving the Ministry of Justice and Safety, the Ministry of Internal Affairs and the National Privacy Authorities (Kanters, 2018). The discussions are centered around the issues of data ownership. In principle, the citizens are the owners of their data and the companies must comply with the requirements of foregoing the ownership in public space of Eindhoven. Transparency and accountability are the standards that guide the open data principle. In order to ensure the data safety on technical and organizational aspects are well executed, it is crucial to

[3] See at https://data.eindhoven.nl/pages/home/

determine the transparency and accountabilities of the partners. Eindhoven smart city projects all strive to comply to the open data standard that is non-intrusive and open (Kanters, 2017). This means that the partners need to facilitate a transparent data processing that can be examined. However, at this stage, this level of transparency is more of a requirement to the public partners than to the private partners. Interviewee 1 stated that data ownership has been difficult to settle with the private partners since the beginning of the project. Philips eventually agreed to the open data principle, which is also one of the companies that only wants to sell the services and doesn't want to own data form the smart lighting initiatives in the smart lighting projects.

The Brainport smart district is an example of initiative that aims fulfill the open data principle for an intelligent and sustainable community completely, given time in ten years. The project is developing from the ground up, cooperating only with partners that can hold up to the privacy standards (Interview on 27 June, 2019). However, the revolution of data ownership in the technology industry is admittedly not a straightforward path, nor can the business model of data mining change immediately. For smart city projects that are expected to deliver service in the short future, it is necessary to be pragmatic about open data principle for optimal quality of the service. In smart mobility programs, Interviewee 6 pointed out that it is not achievable to simply request all commercial partners to share all data they collect and open them up. For example, the project of ember mobility offered reductions for the parking permit for their shared automobiles in exchange of their parking data (Interview on 4 July, 2019). Sometimes, it is necessary to compromise the standard of open data in order to obtain satisfying quality of data. This is shown in the project called secret lama where automobiles equipped with cameras are needed to drive around the city to collect timely data. Complying with the open data principle unconditionally is a direct contradiction to the company's business model. Unless the project compromises to take a free Google service which is not timely or accurate enough, it has to be accepted that some data provided by third parties cannot be made open (Interview on 4 July, 2019). It is notable from this example that the implementation of open data principle might never be complete in today's business model of internet companies.

One important aspect of open data principle is to proactively inform the citizens about the data gathering. Citizens are informed of the development of the projects, as well as how their data are being used. Stratumseind put the business owners and residents on the street at the center stage of

the decision-making (Ollongren, 2017). The citizens and visitors going to Stratumseind can see visible signs of the smart lighting and sound experiment being conducted. The partners that collect data are responsible to inform the subjects of the data collection of what and how their personal data[4] are being collected.

Another aspect of open data principle is to organize the data so that it is open to access and repurposing. One of the main propositions of Stratumseind 2.0 is to create an open data library to achieve data gathered. It is to achieve transparency and open data standard set by Eindhoven smart society vision. The Stratumseind 2.0 project is exploring for maximizing the usage of the anonymous datasets. Interviewee 1 pointed out that the sensors on the Stratumseind street are collecting a large amount of data that are way more valuable than what is currently being analyzed. However, not very project sees the extensive data gathering as an opportunity. The data gathered in smart mobility projects is decided based on the system's functionalities. Whereas data gathered in the smart lighting projects is based on the needs of residents. The goal of a project guides the focus of privacy issues. The smart lighting projects in Eindhoven has no intention to gather all the data that are possible to collect just for the sake of data mining. The data that smart lighting projects gather solely depends on the solutions they aim to provide. Therefore, only data necessary for enabling the project functions will be gathered.

In order to achieve the open data principle, a privacy by design strategy is developed for Eindhoven smart city projects (DITSS, 2017). This principle is demonstrated with the example of the Stratumseind 2.0 project. It was stressed in the interview that the project applies the privacy by design strategy on organizational level, as well as engraved into the technological designs. First, the projects define the technologies and infrastructure that will be applied. This includes identifying the context of the project, the aim of the project, the required functionalities and technologies, as well as the partners that will realize these functions (Ollongren, 2017). For example, in the Stratumseind 2.0 project, the municipality of Eindhoven and DITSS defined that this project is a living lab, which serves as a testing ground and a pioneer for other smart city projects. Since public and private partners are orientated towards different goals, it is important to

[4] Personal data is defined by GDPR as any information relating to an identified or identifiable natural person, including the telephone, credit card or personnel number of a person, account data, number plate, appearance, customer number or address. (GDPR General Data Protection Regulation: Personal Data. 2016) Retrieved from https://gdpr-info.eu/issues/personal-data/

discuss and decide on the methods and manners of gaining the compliance from the private parties during the process of negotiation. Together with a private partner Atos, Stratumseind 2.0 project combines big data analysis and real-time analysis of the data collected on the street for integrated smart crowd management. Atos is responsible for carrying out analysis of data from the sound sensors, image sensors and social media. Based on the analysis, Atos creates profiles of specific situations, such as street fights, by recognizing the patterns of data. This profile then can be used to identify unsafe situations on the street and alert the police of possible violent conflicts on the pub street. The City Pulse pilot then creates a predictive system that strives to prevent street violence from escalation. Defining the data to be collected and used in the big data analysis is the first stage of privacy by design strategy. The goal of City Pulse is clearly defined to be maintaining the public safety on Stratumseind street with a proactive and predictive system enabled by big data analysis (Atos, 2015, p. 1).

The second stage of privacy by design strategy is to set up a system architecture to support the fulfillment of system function and the open data standard at the same time. As mentioned before, the partnership with the national police in the Stratumseind 2.0 project calls for a closer look at the privacy by design strategy (Interview on 22 October, 2018). While the living lab provides research and innovative solutions and the City Pulse pilots provides big data and real-time analysis, the police force requires timely results of the previous two partners to react on. Not only so, the national police are also eligible to a higher level of access to personal information in case an investigation is needed. Eindhoven answers this challenge with a context broker, a strategy to custom the information output according to the designed functions. This way, data is managed as pre-defined datasets and only permitted information will be shown to the relevant partner. It means that the actions that partners can perform are well defined, and likewise, the boundaries of limitations and responsibilities are clear. Such use of context broker is embedded into the organizational arrangement as well as the system architecture. On the organizational level, ranges of access to personal data are defined according to the open data principle and in compliance with GDPR. In the system architecture, the sensors for data collection are designed to transmit only the output that is suited for the context.

The system architecture is also ensured by pre-defining the input of the data analysis. In the Stratumseind 2.0 project, the sound analysis is provided by a private company Sorama with its

sound imaging system. The system monitors the sound level and pattern to sketch the mood of crowd on the street, which in turn, helps to identify a violent conflict. The counting of visitors is achieved through cameras on the street provided by another private partner ViNotion. The company creates and supports a system to detect movements for counting then anonymizes the image of individuals walking for output. Similarly, the cameras to monitor and analyze the flow of cyclists do not outline the identifiable persons (Interview on 22 October, 2018).

From an organizational perspective, privacy by design is followed by the public and private partners of Eindhoven smart city projects, who are responsible for building technologies that follow this strategy (Interview on 21 May, 2019). In this way, privacy by design is implemented in the public and private layers of the system. Overall, smart mobility projects in Eindhoven consider the privacy concern significant in the discussion of cybersecurity. The open data principle is held to be high priority. It is present when a past attempt to achieve cycling traffic tracking was dismissed because it was not possible to develop a satisfactory software for that purpose without creating and tracking personal profiles.

To summarize, privacy concern is highly emphasized by Eindhoven smart city projects. Complying to the privacy first and open data principles, the projects address this concern in two aspects: organizational approaches and technical approaches. Organizationally, the projects ensure that the privacy standards are met by stakeholders through negotiations in the contract phase and through financial compensation for open data. Technically, the projects construct system architecture with privacy by design so that sensitive data cannot be accessed by unintended parties.

4.2 Additional Measures Identified

During the interviews, cybersecurity concerns other than the seven domains established in the theoretical framework were noticed during the interviews. They also pointed out the measures that were taken to prevent potential security breaches caused by these concerns. The following measures of cyber risk and vulnerability will be analyzed: data management and the living lab model.

- Data management

It emerged during the discussion of privacy concerns, that high privacy standard is not only aiming to realize the open data vision of Eindhoven, but also to ensure the quality and the safety of data. When cooperating with multiple stakeholders for data collection, data management comes to be an important discussion of the projects. The data quality is especially focused by projects requiring real-time data analysis. The main cybersecurity of floating car data program for real-time traffic management is the quality of the data. Particularly, the accuracy and stability of the data. Five years ago, Rijkswaterstaat began to examine the possibility of integrating traffic data collected by private companies into the traffic management system. They tested the quality of the data collected by private companies for two years in regards to the stability and accuracy of the data. The conclusion was that these data are good reliable data that can achieve 99.9% accuracy. Yet, there are still improvements needed to start the implementation. The lag of data collected by private companies, such as TomTom, are generally between three to four minutes. However, real-time traffic management demand data that is no more than ten seconds old. Therefore, the data quality standard of the cooperating private companies is being requested to improve. Currently, a pilot program is running to test the ground for future implementation. The cameras on the street of Strijp-S are designed in a way that they can cross-check each other for optimal accuracy, which is as well a measure to improve data quality (Presentation by Strijp-S, 2019).

Another facet of data management is the concern of data safety. “It is impossible to guarantee 100% cybersecurity”, said by Interviewee 4. For Brainport smart district, the quadruple helix is an important measure to counter this challenge. The data team of Brainport smart district is organized by the university. At the early stage of the living lab of the Stratumseind 2.0 project, there was found some vulnerabilities regarding data safety. The system used to blur out the faces of the crowd in the images gathered by the street cameras. The dashboard in the lab can see the image with blurred faces (Atos, 2015). The sound sensors used to gather geological information of the noises and the specific noise level. Both methods were exposing some type of personal information. It was even possibly retraceable to reveal more private individual data. Meanwhile, data safety is challenged to ensure that data can only flow in the intended direction carrying content that is customized by context brokers. For instance, the information that is intended for the police to receive should only be sent to the police. Therefore, changes were made to improve the data safety by applying the privacy by design strategy. As a result, the counting cameras now only output the numbers instead of images of people. Meanwhile, the sound sensors now can recognize the sound

pattern and output the analysis of characteristics of the noises only. It can be concluded that in this project, data safety is managed through design in the system architecture.

System architectures are built to security the data management process by separations of the systems. “The data which we collected from our smart city projects, they are in a separate platform from our regular business”, said Interviewee 2. She explained the system architecture which is consisted of layers to store information and firewalls to protect the layers. This architecture, in turn, prevents the risk from cascade effect by strengthening the system isolation.

- Living lab: learning by doing

Living lab is an experiment embedded in the daily urban life. It is a process of co-creation where the government, citizens, private companies and the research institutes can learn from the testing experience for evaluation and improvement. It is presented as a revolutionary solution to the difficulty of linking the developing innovative systems to the real needs of the society. By combining the stakeholders into an interactive continuous innovation process, Eindhoven smart city projects aim to increase the effectiveness and value of the innovations considerably. This research has assessed the living labs of Brainport smart district, Strijp-S and Stratumseind 2.0 project in previous sections. A living lab generally focuses on limited area packed with various functions for intensive learning. Stratumseind 2.0 project is a good example of this open innovation model. Stratumseind in Eindhoven is one of the busiest pub streets in the Netherlands, which is also known for its level of drunken behavior and frequent fights. The image of aggressiveness on the street has discouraged visitors to go out at Stratumseind. With the purpose of providing a safer nightlight, a living lab has been set up in at Stratumseind, making Stratumseind one of the “smartest” streets in the Netherlands (Naafs, 2018). Aided with WIFI-trackers, cameras and microphones embedded in the lampposts, the living lab can detect aggressive behaviors and alert police department. By experimenting with changing light intensity and colors, the living lab attempts to alter the mood of people when they come out of the bars. Another experiment is to diffuse smells that are supposed to calm the people down. Meanwhile, crowd data is being collected and stored to measure visitor numbers, where visitors come from and go to, are the visitors on foot or cycling, the effect of light and different kinds of sound. That software is now so precise that the Stratumseind living lab and the police are ready to test applications in real life.

However, according to Interviewee 5, the living labs usually have more functions, but they are tailored to that lab which makes it hard to expand (Interview on 28 June, 2019) for the reason that there is no supporting software outside the scale of the living lab. This is confirmed by Interviewee 2, the CIO of municipality of Eindhoven, who stated that living lab "is very difficult to scale up" (Interview on 21 May, 2019). The municipality of Eindhoven is making the effort of transforming living labs to stages of projects. For example, Stratumseind 2.0 project to city center living lab transformation (Presentation by Kanters, 2019), which provides more chances of bringing them to practice.

In contrast, smart lighting projects present a different approach in solving this issue. In the process of learning by doing, smart lighting projects focus on building long-lasting infrastructures in the pilot areas rather than running living labs. Pilot projects start more ground-up. They develop with continuous open innovation to apply software on top of the newly built infrastructure. Smart lighting projects aim to build commercialized platforms that can provide long-lasting support to future innovations. As an example, Heijmans constructed "future proof" intelligent lighting system in Eindhoven that is compliable to applications and software that will be implemented (Interview on 28 June, 2019). In such manner, the smart lighting projects reduce the risk resulted from legacy systems issue. More importantly, it gives the project a better chance of broader implementation. To conclude, learning by doing by means of living lab gives the projects the opportunity to test more innovations. Learning by doing in ways of pilots, on the other hand, provides long-lasting infrastructure for continuous innovation. Both methods provide a testing period for the projects to better understand the cybersecurity issues.

To summarize the analysis, all seven dimensions of smart city risk and vulnerability are considered by the smart city projects in Eindhoven. Of which, the multi-stakeholder dynamic and privacy concern are given most attentions. The discussions regarding weak software security and data encryption, system and maintenance insecurity and risks from the complex attack surface are not neglected. In varying level, measures are implemented by the projects to manage these dimensions of risk. Cascade effect of interrelated systems is not really concerned in the sense of cyberattacks. It is managed mainly in the sense of data management. The human error dimension is least attended to by the smart city projects. The conclusion of the results will be presented in chapter 5.

Chapter 5 Conclusion

This research investigated the cyber risks and vulnerabilities that are concerned by the smart city projects in Eindhoven and the measures that are applied to prevent and mitigate cyber insecurity. By testing against an established theoretical framework, the analysis demonstrates how the theoretical framework can explain the measures taken by Eindhoven smart city projects. Meanwhile, the cybersecurity policies and approaches outside the theoretical framework are presented which can contribute to the development of the framework with empirical evidence.

To answer the research question: *How do smart city projects with open innovation characteristics prevent and mitigate cyber risk and vulnerability?*, it is necessary to answer the sub-questions: 1).*What risks and vulnerabilities are concerned by Eindhoven smart city projects?* 2).*What policies and measures do Eindhoven smart city projects apply to prevent or mitigate cyber risks and vulnerabilities?*

It can be answered that: 1). The projects in Eindhoven are aware of and concerned with the seven dimensions of cyber insecurity put forward by the theoretical framework. However, not all concerns of risk and vulnerability are given equal priority or attention. In line with the theoretical framework, the most concerned cyber risks and vulnerabilities are multi-stakeholder dynamic and privacy concerns; 2). The cybersecurity measures applied in Eindhoven are tailored to prevent risks outlined in the theoretical framework. However, more structured and focused efforts are dedicated to addressing privacy concerns and managing the data flow among the partners. Additionally, cybersecurity measures beyond the ones identified in the theoretical framework emerged during the empirical data gathering. The next paragraphs will address these conclusions.

Different level of consideration of cybersecurity is the result of different focuses of the project. Each project is technologically optimized for its own functions and focuses. For living labs, its primary aim is to speedily realize as much innovations as possible and to test how well they function before full implementation, such as the Stratumseind 2.0 project. The scale of a living lab is usually manageable for a small team which means that cyber insecurity is unlikely to cause great deal of damage. Therefore, less attention is paid to preventing cyber risks and vulnerabilities. The

results show that Eindhoven smart projects have to various extent covered all dimensions of cyber risk and vulnerability from the theoretical framework. However, limited attention was given to the risk and vulnerability of human error. The projects lack of a dedicated cybersecurity team and the municipality can only provide one cybersecurity team for all the projects to share. Interviews suggested that cybersecurity team is not established in every project due to being early in the development stage. The policy instruments of Eindhoven smart city advise not to standardize technical architecture or to reduce the optimizations of each project so that the projects can make more progress and generate more opportunities. However, the cyber insecurity does not only impact the project from the later stage of implementation. Leaving cyber concerns unaddressed can make it challenging to manage when the system is implemented on a larger scale. Therefore, this research suggests that a cybersecurity team should be incorporated into the system design from the beginning, as part of the approach of learning by doing. Only by learning from dealing with contingencies caused by human errors from the testing period, can the project be truly prepared for it in the implementation stage.

The primary focus of cybersecurity dialogues is regarding privacy and the multi-stakeholder dynamic. The discussion of privacy concerns circles around the ownership of data, the accessibility of data and the role of municipalities in managing data. The guiding thread in the strategies is the importance of openness and communication. Through negotiations with the partners and privacy by design, the projects make this openness a tangible concept to implement. The quadruple helix model is introduced as an answer to the multi-stakeholder dynamic, which safeguards the cybersecurity with organizational approaches.

Additionally, two measures can be contributed to the theoretical framework of cyber risk and vulnerability: data security and learning by doing approach. Concluded from the analysis, new indicators presented in the case study of Eindhoven smart city projects are Privacy by design strategy, living lab model and quadruple helix. Eindhoven smart city projects consider the data insecurity a significant risk to the projects, which includes the data quality and safety. It is notable that there are collective efforts to ensure a standard of cybersecurity management. The municipality has a focus on the cybersecurity concerns and pays attention to building appropriate mechanisms. The projects develop system architectures and innovative strategies to data

management. Meanwhile, the open innovative model of living lab creates new opportunities to face the challenge of cybersecurity management.

Discussion

The analysis points out the cyber risks and vulnerabilities identified by previous literature that apply to the current reality in smart city with open innovation characteristics. The results indicate that all seven dimensions of smart city cyber risk and vulnerability are reflected in the projects design. Two dimensions are in line with the theoretical framework. The zero-day exploits are mitigated by implementing hacker team, testing period with living lab model and the negotiation regarding partners' security standards. The cascade effect is managed with the effort to secure the isolation between the systems and the pathways through which data flows. This is in line with previous research of Kitchin & Dodge (2017) included in the theoretical framework.

Some dimensions are managed in different manners than presented in previous research (Cerrudo, 2015; Kitchin & Dodge, 2017) which is due to the open innovation feature of the city. The insecurity resulted from legacy systems is mainly avoided in Eindhoven smart city projects due to its effort to construct new infrastructure, rather than layering innovations to old systems. End-to-end security is recognized by the projects, but it is mainly managed by the partners, which deviates from previous research. The previous research stresses the importance of cybersecurity team for managing this risk (Kitchin & Dodge, 2017). The projects in Eindhoven, on the other hand, entrusts the end-to-end security mainly to the private partners. Unlike pointed out in previous research, human error is given limited attention in Eindhoven smart city projects. Two other dimensions not only reflect previous research but also present more extensive solutions than included in the theoretical framework. The analysis highlighted the particular cybersecurity concerns of privacy and multi-stakeholder dynamics which is in line with the research by Elmaghraby (2014) and Bekara (2014). The projects demonstrated the measures that are tailored to its open innovation features, which are privacy by design strategy and quadruple helix model. These measures are results of Eindhoven's emphasis on achieving a smart society of open innovation. Striving to follow the open data standard and privacy first principles, the projects were motivated to search for solutions that can incorporate all stakeholders yet make sure the data is only accessible to the intended partner. It is thus, meaningful for future research to investigate other smart cities with

open innovation features in order to conclude whether these unique solutions from Eindhoven can be generalized.

Due to the feasibility of this thesis, it is necessary to consider the limitations resulted from the research design and data collection. The first limitation is that it was not feasible to interview all the experts involved in cybersecurity in these projects. This research has attempted to reach experts involved in strategy development, policymaking and the technological departments of the projects. However, most experts who accepted the interview requests are involved in the organizational level of smart city development. This resulted in the extensive measures provided in organizational perspective and less extensive discussions in technical perspective. It is possible that some aspects of cyber security are managed by certain experts but not focused by the project leaders and strategic advisors. This limitation can only be minimized with a much larger research scale. The confirmation bias and political agenda should also be concerned with the results from elite interviews. It was noticed that due to the policy emphasis on the privacy principle and quadruple helix model, the interviewees turn to reveal more information on the dimensions of privacy concern and multi-stakeholder dynamics.

The second limitation is resulted in imbalanced amount of data gathered from each project. It is warned with caution that when conducting such an embedded single case design, much attention needs to be given to the balance between the analysis of the subunits and the research at large (Yin, 2003, p. 46). It is thus, important to make sure that the projects provide relatively even information to the research. Despite the effort to meet this standard, this research cannot ensure the same amount of data gathered from the projects being analyzed. Projects that have been developing for longer period and have been given more publicity are analyzed in greater detail, such as the Stratumseind living lab. This research was able to gather data from multiple visits to the project as well as public documents. In contrast, data regarding the Strijp-S project was only accessible to this research through a short visit to the projects and a presentation by the project leader. Therefore, it is important to understand the result of this research is not a comprehensive summary of the entire smart society development in Eindhoven.

The third limitation is a single-case research design which means that further generalization to other smart cities with open innovation features cannot be made.

Learning from the limitations of this thesis, research suggestions that can further the understanding of this research are made. A similar in-depth single case study could benefit from including data from the technical and organizational aspects in a more evenly distributed way. The technological experts of cybersecurity in the smart city projects should be given equal attention as the policymakers. That being said, future research could also be valuable if it can separate the technical and organizational aspects of cybersecurity in its research design and then deepen the knowledge on either one of the aspects. Furthermore, future research can benefit from engaging the projects in a more balanced manner if a single case of a city is chosen. It is also advisable to look into smart city projects that are in the same phase of development, which might present more consistent cybersecurity focuses. If aiming for conclusions that could be generalized to more cities, a comparative case study is the suggested method. Cities with similar open innovation characteristics can be tested against the smart city cybersecurity theoretical framework together. By examining whether all cities with open innovation features share similar cyber security concerns and whether these cities apply similar measures, it is possible to generate generalized conclusions to the research question of *How do smart city projects with open innovation characteristics prevent and mitigate cyber risk and vulnerability?*

Based on the findings of this research, this research makes practical suggestions that Eindhoven smart city projects might benefit from. It is concluded that there is a lack of focus on establishment of cybersecurity team within each project, which is crucial in preventing risks from human error and zero-day exploits. This research finds that the smart city projects can improve by engaging more discussions of dedicating cybersecurity management within each project from the early stage of project development. By doing so, when the opportunities emerge for the projects to expand to larger scales, the strategies will be ready to ensure a stronger cybersecurity resilience.

Acknowledgements

I would like to express my appreciation to the experts from municipality of Eindhoven and the living labs in Eindhoven for the interviews and visits to the projects, making it possible to conduct this research.

I thank my supervisor Dr Vlad Niculescu-Dincă for your advices and the introduction to the interesting topic of Eindhoven smart city.

My sincere thanks also go to Anouk and Renske for reviewing my thesis and providing helpful insights.

With special gratitude, I thank my parents, my partner and my family for all your support during the endeavor to complete this thesis. It would not have been possible without you!

Bibliography

Alba, D. (2015, 01.27.15). The FTC Warns Internet of Things Businesses to Bake in Privacy and Security. Retrieved from https://www.wired.com/2015/01/ftc-warns-huge-security-risks-internet-things/

AlDairi, A., & Tawalbeh, L. (2017). *Cyber Security Attacks on Smart Cities and Associated Mobile Technologies* (Vol. 109).

Almirall, E., Lee, M., & Wareham, J. (2012). Mapping living labs in the landscape of innovation methodologies. *Technology innovation management review, 2*(9).

Andersson, G., Donalek, P., Farmer, R., Hatziargyriou, N., Kamwa, I., Kundur, P., . . . Sanchez-Gasca, J. (2005). Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance. *IEEE transactions on Power Systems, 20*(4), 1922-1928.

Atos. (2015). Atos uses Big Data analytics for safer streets. Retrieved 21 July, 2019, from Atos Group https://atos.net/en/2015/press-release/general-press-releases_2015_07_21/pr-2015_07_21_01

Aven, T. (2007). A unified framework for risk and vulnerability analysis covering both safety and security. *Reliability Engineering & System Safety, 92*(6), 745-754. doi:https://doi.org/10.1016/j.ress.2006.03.008

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., . . . Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation, 22*, 3-13. doi:https://doi.org/10.1016/j.diin.2017.06.015

Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., . . . Portugali, Y. (2012). Smart cities of the future. *The European Physical Journal Special Topics, 214*(1), 481-518. doi:10.1140/epjst/e2012-01703-3

Beatty, M. E., Phelps, S., Rohner, C., & Weisfuse, I. (2006). Blackout of 2003: Public Health Effects and Emergency Response. *Public Health Reports, 121*(1), 36-44. doi:10.1177/003335490612100109

Bekara, C. (2014). Security Issues and Challenges for the IoT-based Smart Grid. *Procedia Computer Science, 34*, 532-537. doi:10.1016/j.procs.2014.07.064

Bennett, A. (2004). Case study methods: Design, use, and comparative advantages. *Models, numbers, and cases: Methods for studying international relations*, 19-55.

Berk, R. A. (1983). An introduction to sample selection bias in sociological data. *American Sociological Review*, 386-398.

Brainport. (2016). *WELCOME TO BRAINPORT EINDHOVEN: Europe's leading innovative top technology region*. Retrieved from WWW.BRAINPORTEINDHOVEN.COM:

Castelnovo, W., Misuraca, G., & Savoldelli, A. (2016). Smart Cities Governance:The Need for a Holistic Approach to Assessing Urban Participatory Policy Making. *Social Science Computer Review, 34*(6), 724-739. doi:10.1177/0894439315611103

Cerrudo, C. (2015). An emerging US (and world) threat: Cities wide open to cyber attacks. *Securing Smart Cities*.

Coe, A., Paquet, G., & Roy, J. (2001). E-Governance and Smart Communities:A Social Learning Challenge. *Social Science Computer Review, 19*(1), 80-93. doi:10.1177/089443930101900107

Depuru, S. S. S. R., Wang, L., & Devabhaktuni, V. (2011). Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft. *Energy Policy, 39*(2), 1007-1015.

Dirks, S., & Keeling, M. (2009). A vision of smarter cities: How cities can lead the way into a prosperous and sustainable future. *IBM Institute for business Value, 8*.

DITSS (2017, August). [Presentation by DITSS].

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review, 14*(4), 532-550.

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

EurActiv. (2013, 5 February). Europe Looks to Tech Hubs to Lure Foreign Investment. Retrieved from http://www.euractiv.com/specialreport-internet-europes-f/europe-lookstech-hubs-lure-fore-news-517569

Gillham, B. (2005). *Research Interviewing: The range of techniques: A practical guide*: McGraw-Hill Education (UK).

Harkins, M., & Freed, A. M. (2018). The Ransomware Assault on the Healthcare Sector. *Journal of Law & Cyber Warfare, 6*(2), 148-164.

Hollands, R. G. (2008). Will the real smart city please stand up? *City, 12*(3), 303-320. doi:10.1080/13604810802479126

Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and open government. *Information systems management, 29*(4), 258-268.

Jin, J., Gubbi, J., Marusic, S., & Palaniswami, M. (2014). An information framework for creating a smart city through internet of things. *IEEE Internet of Things journal, 1*(2), 112-121.

Jokar, P., Arianpoo, N., & Leung, V. C. (2016). A survey on security issues in smart grids. *Security and Communication Networks, 9*(3), 262-273.

Kanters, T. (2019, 26 June). [Presentation by Tinus Kanters].

Khatoun, R., & Zeadally, S. (2016). Smart cities: concepts, architectures, research opportunities. *Commun. Acm, 59*(8), 46-57.

Kitchin, R. (2014a). *The data revolution: Big data, open data, data infrastructures and their consequences*: Sage.

Kitchin, R. (2014b). The real-time city? Big data and smart urbanism. *GeoJournal, 79*(1), 1-14. doi:10.1007/s10708-013-9516-8

Kitchin, R., & Dodge, M. (2011). *Code/space: Software and everyday life*: Mit Press.

Kitchin, R., & Dodge, M. (2017). The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *Journal of Urban Technology*, 1-19. doi:10.1080/10630732.2017.1408002

Lacinák, M., & Ristvej, J. (2017). Smart City, Safety and Security. *Procedia Engineering, 192*, 522-527. doi:https://doi.org/10.1016/j.proeng.2017.06.090

Lu, Z., Lu, X., Wang, W., & Wang, C. (2010). *Review and evaluation of security threats on the communication networks in the smart grid.* Paper presented at the 2010-MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE.

Manville, C., Cochrane, G., Cave, J., Millard, J., Pederson, J. K., Thaarup, R. K., . . . Kotterink, B. (2014). Mapping smart cities in the EU.

Mattoni, B., Gugliermetti, F., & Bisegna, F. (2015). A multilevel method to assess and design the renovation and integration of Smart Cities. *Sustainable Cities and Society, 15*, 105-119. doi:https://doi.org/10.1016/j.scs.2014.12.002

Mead, N. R., Hough, E. D., & Stehney II, T. R. (2006). *Security Quality Requirements Engineering (SQUARE) Methodology*. Retrieved from Pittsburgh, PA: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2005_005_001_14594.pdf

Mohanty, S. P., Choppali, U., & Kougianos, E. (2016). Everything you wanted to know about smart cities: The internet of things is the backbone. *IEEE Consumer Electronics Magazine, 5*(3), 60-70.

Mol, C. K., Osman; Aalders, Rob; Schouten, Nico (2015). *A Spotlight on Smart City Eindhoven: How can Eindhoven become a Smart City faster?* Retrieved from Smart City StarterK!t 1.0:

Naafs, S. (2018). 'Living laboratories': the Dutch cities amassing data on oblivious residents

Retrieved from https://www.theguardian.com/cities/2018/mar/01/smart-cities-data-privacy-eindhoven-utrecht

Nam, T., & Pardo, T. A. (2011). *Conceptualizing smart city with dimensions of technology, people, and institutions*. Paper presented at the Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times, College Park, Maryland, USA.

Neirotti, P., De Marco, A., Cagliano, A. C., Mangano, G., & Scorrano, F. (2014). Current trends in Smart City initiatives: Some stylised facts. *Cities, 38*, 25-36. doi:https://doi.org/10.1016/j.cities.2013.12.010

Ollongren, W. D. W. (2017). *Policy instrument open innovation*. StarterK!t Retrieved from http://switchlight.nl/en/smart-city-starterkit-conditions/.

Ouden, d., P. H. & Valkenburg, R. (2012). *Vision and roadmap urban lighting Eindhoven 2030 : research results July 2012*. Retrieved from Eindhoven: https://pure.tue.nl/ws/portalfiles/portal/3739026/747898.pdf

Owens, W. A., Dam, K. W., & Lin, H. S. (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: The National Academies Press.

Paskaleva, K. A. (2011). The smart city: A nexus for open innovation? *Intelligent Buildings International, 3*(3), 153-171.

Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M., & Oliveira, A. (2011). *Smart cities and the future internet: Towards cooperation frameworks for open innovation.* Paper presented at the The future internet assembly.

Schneier, B. (2017a). Click Here to Kill Everyone. *New York Magazine*. Retrieved from http://nymag.com/intelligencer/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html

Schneier, B. (2017b). The next ransomware attack will be worse than WannaCry. In.

Smith, L. (2018, 02-27). Eindhoven: Driving Open Innovation & Collaboration CITY PORTRAITS. Retrieved from https://hub.beesmart.city/city-portraits/smart-city-portrait-eindhoven

StarterK!t. (2015a). *Open data principles* Switch.nl: Municipality of Eindhoven Retrieved from http://switchlight.nl/en/smart-city-starterkit-conditions/.

StarterK!t. (2015b). *Smart Society Charter. IoT Architecture principles & guidelines*. switch.nl: City of Eindhoven Retrieved from http://switchlight.nl/en/smart-city-starterkit-conditions/.

Strijp-S (2019, 25 june). [Presentation by Strijp-S].

Townsend, A. M. (2013). *Smart cities: Big data, civic hackers, and the quest for a new utopia*: WW Norton & Company.

Triangulun. (2017). City of Eindhoven, Netherlands. Retrieved from https://www.triangulum-project.eu/?page_id=2137

TU/e. (2019). Smart Cities Program. Retrieved from https://www.tue.nl/en/university/departments/built-environment/research/smart-cities-program/research/research-programme/

UN. (2018a). 2018 Revision of World Urbanization Prospects. Retrieved from https://www.un.org/development/desa/publications/2018-revision-of-world-urbanization-prospects.html

UN. (2018b). *World Urbanization Prospects: the 2018 Revision* UN DESA: UN DESA Retrieved from https://population.un.org/wup/Publications/Files/WUP2018-KeyFacts.pdf.

Villani, E., Greco, L., & Phillips, N. (2017). Understanding Value Creation in Public - Private Partnerships: A Comparative Case Study. *Journal of Management Studies, 54*(6), 876-905.

Wu, Y., Zhang, W., Shen, J., Mo, Z., & Peng, Y. (2018). Smart city with Chinese characteristics against the background of big data: Idea, action and risk. *Journal of Cleaner Production, 173*, 60-66. doi:https://doi.org/10.1016/j.jclepro.2017.01.047

Yin, R. K. (2003). Case study research design and methods third edition. *Applied social research methods series, 5*.

Appendix

Appendix I: List of Abbreviations

ICTs	Information and Computing Technologies
IoTs	Internet of Things
ICF	Intelligent Community Forum
TU/e	Eindhoven University of Technology
DoS	denial-of-service
SaaS	Software as a Service
CIO	Chief Information Officer
CERTs	Computer Emergency Response Teams
SCCIP	Smart City Continuous Innovation Process
ICF	Intelligent Community Forum
DITSS	The Dutch Institute for Technology, Safety & Security
API	application program interface
FIWARE	Future Internet Middleware for Smart Cities
GDPR	General Data Protection Regulation
NDW	National Data Warehouse

Appendix II: Interview Framework

The purpose of this research is to understand what cybersecurity risk and vulnerabilities are concerned by Eindhoven smart city projects and how the projects prevent and mitigate yber insecurity. I am responsible for the design and conduct of this interview. This interview will take approximately 45 minutes. I would like to record this interview with your permission. The recording will only be for me to reflect on later.

Question 1:

What do you think are the main cybersecurity concerns for the smart city projects?

Question 2:

What cybersecurity measures, such as regular password change and system updates, are taken against software security?

Question 3:

How do you minimize cybersecurity risk when cooperating with third parties, such as technology and service providers? Are the partners' systems inherently trusted? Who has the data ownership?

Question 4:

How are the systems tested before putting into operation? Are hacker tops employed? How long is the testing period?

Question 5:

How is the end-to-end security in Internet of things maintained?

Question 6:

How do you isolate the security risks among interconnected systems? For example, security attack on one part of the system cascading to another.

Question 7:

Many smart city transformations require applying current technologies to previous existing legacy systems. How do you minimize forever-day exploits in legacy systems?

Question 8:

What does the cybersecurity team look like in Eindhoven smart city projects? What cybersecurity trainings for other employees are provided?

Question 9:

What cybersecurity measures are taken to mitigate the potential zero-day exploits in the system design, such as code errors?

Question 10:

What cybersecurity measures are taken regarding the public and private partnership?

Question 11:

What is the relevance of smart city stakeholders to cybersecurity?

Question 12:

What are the security concerns regarding privacy? What are the measures against these concerns?