Have you updated your lightbulb?

Solving IoT vulnerabilities through governance

TU Delft

Tom de Roon

Have you updated your lightbulb:
Solving IoT vulnerabilities through governance

By

T. de Roon

in partial fulfilment of the requirements for the degree of

Master of Science
in Complex Systems Engineering and Management (CoSEM)
Faculty of Technology, Policy and Management (TPM)

at the Delft University of Technology,
to be defended publicly on Monday July 19th, 2021 at 14:30.

Supervisor:	Dr. S.E. Parkin,	Section O&G, Multi-Actor systems
Thesis committee:		
Second supervisor:	Dr. J. Ubacht,	Section ICT, ESS department
Chairperson:	Prof.dr. M.J.G. van Eeten,	Section O&G, Multi-Actor systems
External supervisor:	R. Krenn,	Cybersprint bv, Den Haag.

Preface

Dear reader,

This master thesis project, titled: *"Have you updated your lightbulb? Solving IoT vulnerabilities through governance*", is written to research the governance involved with solving cybersecurity vulnerabilities in Internet of Things (IoT) devices. It is written to graduate from the Complex Systems engineering and Management (CoSEM) master program at the Technische Universiteit Delft. From the initial research proposal to this final product took from February 2021 till July 2021.

The starting point for this research is the smart city project from the municipality of The Hague, in cooperation with Cybersprint BV. I undertook a graduation internship at Cybersprint BV to get access to IoT data. With an interest in cybersecurity and governance, the research objective and goal was formulated with the help of my first supervisor, Simon Parkin, and committee chair, Michel van Eeten. Executing this research proved to be one of the most uncertain and challenging tasks I ever did at university, especially given the extra boundaries the corona pandemic put on the possibilities of conducting this research.

Through writing this, I would like to thank Simon Parkin for his guidance and always being available on short notice to answer one of my many questions, and to ensure I was making good progress. You always managed to put me on the right track again. Also, thank you to Michel van Eeten for answering any questions I had that Simon was uncertain about, and providing your knowledge and insights about this project. Thank you to Robert Krenn from Cybersprint, for your cooperation, kind advice and information, and help every time I asked for it. The meetings with you were always valuable.

A special thank you to Jolien Ubacht for always going the extra step in providing feedback or answering my emails. You always provided more explanation or feedback than I expected to get. This extra information was mostly unsolicited, and I really appreciated it since it helped clearing up any unknowns or uncertainties.

Even though I hesitated to thank any friends and family this way, I have to thank Scott, Alexa & Stella for asking me how I was doing every other day and genuinely being interested all the time. I was able to discuss every aspect of research and graduation with you, which really helped. Also thank you Tim, for taking me away from my computer every once in a while while saying *'You have to get outside sometimes'*, and getting me to walk on the beach more during the writing of this thesis than ever before.

Last but not least, a thank you to my parents for understanding that sometimes things were not going as planned and providing support.

I hope this research proves itself to be useful, and you enjoy reading it.

Tom de Roon
Rockanje, July 19th, 2021

Summary

Connecting ‘things’ like a doorbell, webcam, lamp, or other objects to the web to provide a service or control is called the Internet of Things (IoT). These devices contain vulnerabilities that form risks for the device user and possibly the network owner through their heterogeneity. The identified knowledge gap is the need for more IoT governance but no specification on governance options and means to reach specific stakeholders. This indicates uncertainties about who to involve and in what way.
Through the smart city initiative of the municipality of The Hague, a cyber security company called Cybersprint has a dataset of network scan data which is used for this research. Using this dataset as the empirical context for the defined knowledge gap, this research aims to look into the vulnerabilities IoT devices carry, and then look into relevant stakeholders to see what they can do through governance and why they are not doing this. To answer the main research question: How can the municipality of The Hague use governance instruments to decrease cyber vulnerabilities in IoT devices?

A literature study of IoT and smart city applications is used to define IoT concepts. IoT is split up into three layers: the application, perception, and network layer. On these layers, different security issues related to IoT devices are described. After defining this basis for IoT related to this research, a literature study is used to define the governance of IoT and current governance examples. These literature studies form the background information for the rest of this research.
The database of 1649 IP addresses of network scan data from the area of The Hague is then used to find what vulnerabilities are present and what stakeholders are identifiable from this data. Exploring this network scan data showed only 191 devices are fully identifiable from the total number of IP addresses. These devices all carry vulnerabilities for the user of these devices, and being visible is by itself a vulnerability. No device owners could be directly identified, only the providers of the networks these devices are found in. This results in the identifiable stakeholders from the dataset: ISPs and device manufacturers.

Based on the identification of device manufacturer, ISP, and municipality as involved stakeholders, a selection of governance options is made. Consisting of informing device users, steering device users, policing IoT, steering ISPs, steering manufacturers, and security-by-design. These options were assessed on viability and validity through semi-structured interviews with three ISPs and the municipality. This showed that the role of ISPs is less relevant than initially described in literature due to legal boundaries and incentive problems. The role of manufacturers is more important, and devices should be standardized and legislated more. According to the interviewed ISPs and municipality, there is no need for more specific IoT data since legislation prevents this from being collected. There is a need to create a better problematization, allowing the involvement of other stakeholders and putting the problem on the national agenda. The collected networks scan data can be used for more quantitative insights and can not be provided by ISPs due to legal restrictions. The current data collected by a third party like Cybersprint seems like the best option for these insights.

The most viable action to take is informing device users since secure configuration and usage of a device would take away vulnerabilities while waiting for European legislation to be implemented. This legislation will force more security-by-design. The recommendation for the municipality is to take the role of leading actor, provide a better problematization with the data available, and use this to generate more urgency with other stakeholders. Starting public-private partnerships (with ISPs, device vendors, universities, other municipalities: different perspectives to progress the problem) and starting information campaigns and therefore try to reach as many people as possible. Even though ISPs can not provide in reaching vulnerable users directly, they can help in general information campaigns. Increasing security practices on the user side while waiting for legislation on the manufacturer's side.

Contents

1 Introduction

1.1. Background

This chapter introduces the research area of the internet of things. A problematization and identification of knowledge gaps will lead to the primary research objective and question.

1.1.1 Buying a webcam

Imagine having a house with a driveway. One night you park your car, and the following day you find something (or someone) scratched your car. Visibly upset, you immediately go to a local store and buy a full HD security webcam. The only thing you need to do is attach it to the side of your house and connect it to your Wi-Fi network. You have to download an application on your phone, add the camera, and now you cannot only control the camera but have a live video feed of the footage. You can also save images or videos to your phone. For only 50 euros it looks like you made a great decision.

You might feel secure, knowing any person walking on your driveway is caught on video. However, unknowingly any person with an internet connection can look at your webcam feed (Visterin, 2016). The 'great deal' you made comes with a price: you compromised your privacy online for a sense of more security around your house. This example is part of the dangers of the internet of things.

1.1.2. The Internet of Things

Connecting networks of university computers to exchange information with each other was the main idea behind 'the internet' (Press, 2015). Since the general introduction of the internet in 1991, ongoing innovations and developments have changed societies' ways. Through the years, more and more devices and objects became connected to the internet. The initial network of homogeneous devices (computers) has turned into a global network of heterogeneous devices.

Defining IoT

Connecting different devices and objects to the internet to create a network is described as 'the internet of things' (abbreviated as IoT). Defined as*: "A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies"* (ITU-T, 2012). The development of the internet of things enabled new uses for the internet. While the internet itself operates optimally through *"automation and reduction of human input"* (Radanliev et al., 2019), it is primarily this human input that makes IoT devices work. IoT relies on information sharing and collaboration between people and people, people and things, and things and things (Lee & Lee, 2015).

Consumer IoT

Applying IoT to consumer devices results in home automation devices (domotics). This gives users remote access or control of household items, primarily using a predefined chain of events that a user starts. For example, turning off all lights when the user shouts, *"Hey Google, turn off all lights".* General consumer IoT devices enhance services and usability by connecting to the internet, like webcams and smartwatches. There is also a focus on connected household devices like doorbells and fridges. These are all part of so-called smart home appliances, which enable remote monitoring and management of technologies in the user's home environment (Loi et al., 2017).

Business IoT

Applying the internet of things on an industrial business level will be mainly directed towards monitoring and control to improve business processes through IoT captured information (Lee & Lee, 2015). Using connected IoT devices within business processes to find areas of improvement and even predict future states of the business process. Within this context, the internet of things is also referred to as: 'the Internet of Everything" (Lee & Lee, 2015) since it relies on machines, devices, and sensors within the whole business process to collect information and communicate, which could also include monitoring production machines to maximize efficiency. However, having a surveillance camera connected to the internet in a retail shop is also considered business IoT.

Smart city IoT

Comprised of both consumer IoT and business IoT, smart city IoT overlaps both and adds the usage of smart city applications by adding IoT in the public space (see figure 1.1). That could be monitoring public areas and using IoT information to inform inhabitants, enforce policies, or inform policymaking. Applications are, among others, monitoring traffic flows, gathering information on how busy areas are, or tracking car parking (Arasteh et al., 2016). Through the smart city concept, public IoT information connects with household IoT information. For example, signalling garbage collection at home when a waste container is full and giving the garbage collector an efficient route to empty all full waste containers (Hammi et al., 2018). Current application areas (among others) are smart transportation, e-healthcare, safety and justice, smart parking, waste management, and smart energy metering (Mehmood et al., 2017). The core concept of these IoT developments relies on accessible, reliable data used in real-time and to support residents (Hammi et al., 2018). Sharing this data results in public and private actors cooperating to provide smart city services to residents. The potential danger lies in connecting seemingly innocent objects and devices to a smart city network. Malicious actors could use the information or network itself for criminal behaviour, such as the Erasmus bridge in Rotterdam that got hacked and changed lights (Verlaan, 2020), which could be a prelude to a real threat involving IoT.

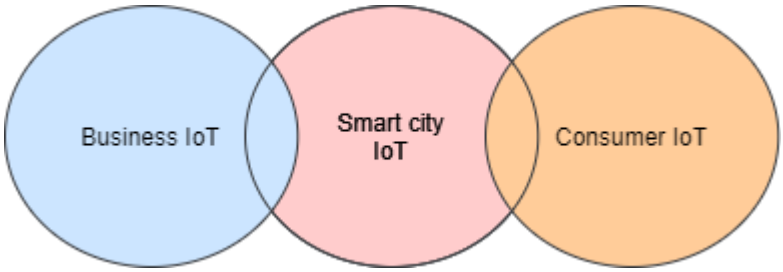

Figure 1.1 The overlap between different application areas of IoT, as defined for this research.

These three areas of IoT highlight the relation between different uses of IoT. They indicate that you can still specify the different sorts of IoT encompassing smart city IoT by taking a smart city perspective. For this research, the takeaway is that by focussing on analyzing IoT (either business or consumer IoT), it will also (indirectly) relate to smart city IoT.

1.1.3. Identifying the problem

The increasing number of IoT devices and application areas make way for innovation and novel means of interaction.

Security risks

There is a probability of some incident occurring for every connected device, harming a single user or an entire network. This risk is defined as: *"the probability that a threat event will occur and result in a negative impact on or harm of an asset."* (Radanliev et al., 2019, p. 2). Any device connected to the internet has the potential to carry a cyber vulnerability that increases the chance of reaching and impacting a potentially valuable asset. More widespread adoption of IoT devices in multiple areas (consumers, businesses, public areas) creates a more extensive surface area for a potential threat event. Malicious actors targeting devices to be infected with malware, infiltrating devices to uncover personal information about the user, or using 'innocent' devices as a means in a botnet are examples of threats. These scenarios involve technology and security risks, but with underlying privacy and primarily ethical risk (Radanliev et al., 2019, p. 3). Privacy risks that result from gathering personal data can result in real-world damages. Imagine a webcam that an intruder can check to ensure no one is home before breaking in, or the ability to inquire sensitive personal data through a cyber vulnerability could result in criminal behaviour or a loss of money. Therefore the broader type of risk for this research will be defined as 'cyber risk', being: *"Any circumstance or event with the potential to adversely impact (…) individuals (…) through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service"* (NIST, 2015).

Societal issues

Increasing use of IoT affects users as well as to non-users of IoT. Potential business opportunities related to the adoption of IoT will affect human behaviour. Smartwatches changed into a means for payment by giving the option to pay with a smart device, for instance. In this sense, the internet of things is an evolving socio-technical ecosystem formed by heterogeneous devices and objects. The result is a large scale complex network that has to balance innovation and progress versus security issues and risks. Within the area of IoT, there are different stakeholders with different perspectives. Users of IoT devices consist of consumers, businesses, public stakeholders, manufacturers of the IoT devices, but also internet service providers that provide an infrastructure for IoT devices to function.

For this research, the term 'user' is defined as any person or organization using an IoT device. This definition is not limited to single consumers or private users but also public stakeholders. This results in businesses seeking innovation and making profits through their business models while the government must safeguard the security and protect shared values. The main instrument for managing this would be using so-called governance instruments.

Governance

Technology does not operate by itself in an isolated manner. Technology in society becomes a so-called socio-technical system, which is defined as an interaction of social and technical areas, that "*have developed specific forms of collective knowledge production, knowledge utilization and innovation, and which are oriented towards specific purposes in society and economy"* (Borrás & Edler, 2014, p. 11). This interplay between technology and society operates on governance, which is defined as: *"The action or manner of governing (something)."* (IT Governance Institute, 2013). This is expressly defined to include rules and regulations, but also social agreements and non-textual agreements between parties. Therefore in this research, governance is defined as any form or agreement to rule or control the socio-technical system of IoT.
From this general governance aspect, you can create specific governance instruments. A 'governance instrument' is defined as an overarching term consisting of policy instruments that belong to state actors and social instruments that belong to non-state actors (Borrás & Edler, 2014)—indicating a multi-actor perspective between public and private actors.

1.2. Research gaps

An exploration through literature will result in the specific knowledge gap that is researched. This knowledge gap will lead to a central research objective and question.

1.2.1. Literature search

A literature overview was used to identify research gaps in the field of IoT security and governance. After an initial exploration with Google Scholar, SCOPUS was used as the main database for literature. The search terms for this were: *the internet of things AND security AND governance*, with deviations using synonyms and abbreviations (like *IoT*) and adding *users* or *cyber security* as search terms. Papers are selected based on the amount of citations, since highly cited papers could indicate more scientific relevance (Aksnes et al., 2019). Also the abstract was read to decide on the relevance, based on how the paper addresses IoT issues in relation to governance. This resulted in thirty-two papers with delineations ranging from specific IoT technologies to more general IoT overview papers. These resulting papers were a selection of highly cited papers, but also relevant more recent papers with little citations but applicable to this research (based on reading the abstract).

The criteria for elimination were the applicability of the abstract concerning issues relating to governance and Iot, and then the number of citations between similar papers. In this case more citations are better. This resulted in 17 sources of literature used to identify a knowledge gap. An overview of these papers can be found in Appendix A: The knowledge gap.

1.2.2. General literature on IoT security

There is a focus on general IoT within the literature, with no emphasis on specific concepts or technology. This gives a sense of the most prevalent security issues in IoT devices. The most significant overall challenge is privacy (Gupta & Shukla, 2016): Monitoring every IoT device would be most secure while also violating privacy. Zhao & Ge (2013) and Alaba et al. (2017) add to this by looking at IoT security in general and concluding that the heterogeneous nature of IoT makes it difficult to control different devices and can be seen as a barrier for making different hardware and software objects work together. Lastly, Alaba et al. (2017) note that the combination of protocols and rules is missing in current IoT developments, indicating a lack of consensus in managing. These general IoT reviews seem to lack specificity in terms of solutions to security issues.

Babar et al. (2011) specify that IoT security needs to start at development and be thought through till deployment. A lack of standardization hinders IoT development (Miorandi et al., 2012). Authentication standards, together with regulations about tracking actors within an IoT network (Riahi Sfar et al., 2018), as well as more compliance with existing laws, is also lacking (Singh et al., 2016). This relates to more transparency and indicates that mechanisms like contracts and trust between different stakeholders (like manufacturers, sellers, authorities, and ISPs) in IoT fall behind.

On the user side (consumers, businesses), security issues are prevalent but dependant on the perceptions of these users. Issues perceived on the user level drive regulations (Zeng et al., 2017). Most users seem either unaware or indifferent about security issues mostly involving their privacy (Hsu & Lin, 2016). Privacy is valued, but users do not look into security information provided by an IoT manufacturer (Emami-Naeini et al., 2019). IoT devices should inform any bystander of possible privacy infringing information gathering before subjecting a person to this threat (Marky et al., 2020). This relates to remediation solutions starting at the user level (resetting a device, updating a device, etc.) presented as solutions (Tejasvi Alladi et al., 2020; Pishcva & Takeda, 2006). From these, no tangible ways to reach the user level seems defined. This can be described as a lack of research that is *"aware of, and involves the user",* adding that *"most IoT device owners are not security experts, it is necessary to devise novel forms of communication of security findings which are accessible to this population"* (De Carli & Mignano, n.d.). There should also be more standards defined within the IoT industry and legislators and policymakers to protect users (Loi et al., 2017). Responsibility is given to the user.

Remediation efforts highlight similar issues, given the case of researching the Mirai botnet that infects IoT devices. Once specific IP addresses of infected devices are found, there seems to be a lack of information on device owner identification and communication channels to provide actionable notifications (Cetin, Ganan, Altena, Kasama, et al., 2019; Cetin, Ganan, Altena, Tajalizadehkhoob, et al., 2019). Using internet service providers as the main responsible stakeholder to reach infected device users or owners, these internet service providers seem to have weak incentives to notify IoT users based on vulnerabilities found (Cetin, Ganan, Altena, Kasama, et al., 2019). This indicates stakeholders with different roles but a lack of information on what data is available and who should (and is allowed to) act on this data, again putting the responsibility at the user.

The identified research gap

Security solutions in IoT are described through numerous specific technical interventions, while governance solutions mostly contain a general aspect. An overarching element in literature is the lack of specification within this governance aspect (see Appendix A: The knowledge gap). A multi-stakeholder perspective is often indicated, but relating this to implementing governance highlights the issue of control. Giving an authority access to all required data to solve security issues will infringe on user privacy, for instance. The analytical blind spot sits between knowing IoT vulnerabilities and reaching the correct stakeholders to act on this security issue. The main problem then becomes identifying the involved issues, involved stakeholders, and finding out what governance can be implemented to solve these security issues. This also places the issue away from single users and more towards a multi-stakeholder perspective: since you can say security needs to be fixed at users, but having no specification on how to involve these users means the responsibility lies with another involved party.

1.2.3. Identifying the problem owner

The application area that involves the consumer, business, and public side of IoT is the development of smart cities. This area of IoT development will be used for the defined knowledge gap. Private stakeholders directly work with citizens within smart cities, but smart city concepts are financed and arranged by public stakeholders. For smart cities, this is defined as a so-called *"primus inter pares"* governance mode (Borrás & Edler, 2020), and public-private interactions are needed to ensure governance (Borrás & Edler, 2014). For smart city initiatives in the Netherlands, this main stakeholder is a local municipality since it is expected that they have a voice and capability to deploy governance instruments.

1.3. Smartcity The Hague and Cybersprint

The defined research gap is broad and general by itself. The context for this research will be the city of The Hague, through their smart city initiative. The city of The Hague has the ambition to develop itself as a smart city. They want to ensure a safe digital environment for its citizens, facilitated by the municipality (Gemeente Den Haag, 2021; *Smart City Den Haag* , n.d.).

This ambition led to a cooperation with Cybersprint, a cybersecurity company specialized in attack surface monitoring. They scan, identify and monitor online systems for other actors. Cybersprint is a third party, meaning they are a private actor serving private or public actors. Through the data they collect Cybersprint can identify vulnerabilities and security issues, and also identify IoT devices within the networks they scan. They do not provide these networks (like an internet service provider). Through a partnership with the municipality of The Hague, Cybersprint uses their own infrastructure to scan the networks of the city of The Hague and provide data on IoT devices in a data portal. This data is used as input for this research to ground the conclusions in a real-life context.

1.4. Main research question

This research studies the defined knowledge gap through empirical data from the area of The Hague. Therefore the research objective is defined as:

Finding governance instruments that have the ability to reach relevant stakeholders and, through this, decrease cyber vulnerabilities in IoT devices.

By looking into this research objective, a synthesis of information will lead to answering the following main research question:

How can the municipality of The Hague use governance instruments to decrease cyber vulnerabilities in IoT devices?

This research aims to define a conceptual framework consisting of different stakeholders involved resulting from the network data of The Hague and literature, different types of governance instruments, and the barriers to implementing these options. Using the options of all defined stakeholders involved, this research will conclude with the next steps the municipality of The Hague can take to involve the right stakeholders and decrease cyber vulnerabilities in IoT devices.

1.5. Research outline

This research aims to use empirical data to find out what security issues are found in public IoT networks, identify what stakeholders are involved in this, and what options there are for these stakeholders to solve IoT vulnerabilities and see why they are not doing this.

To understand the current setting and aspects of IoT networks and look into governance, the first step is to conduct two literature studies. First, a literature study into the characteristics of IoT itself and relevant security aspects and issues. The second literature study will be into governance characteristics and instruments.
The next step in the research will be to use the IoT data of The Hague to provide the context for further research. This means looking into characteristics of network scan data, defining what IoT devices are present, and finding what can be identified from network scan data. Based on this context, specific stakeholders will be identified and used to determine the governance options. These options will be validated, and through a synthesis of the literature outcomes, data exploration, and stakeholder identification result in a conceptual framework. The possible options and barriers that stop the implementation for all identified stakeholders will become clear from this framework.
For the conclusion, the outcome will be generalized to answer the main research question. The methodology to derive an answer to the main research question will be addressed in the next chapter.

2 Methodology

In this chapter, the research methodology is addressed. The area and use of mixed method research will be highlighted and argued for through the starting point of qualitative and quantitative research. Different sub-questions will be defined through this approach, and the relevance within this research will be shown. These research questions will provide an answer to the main research question, and therefore the research objective.

2.1. Mixed method research

For this research, literature reviews into IoT and governance define the conceptual foundations and find relevant literary concepts. After this, quantitative data is used to determine the empirical context for the follow-up questions and back-up qualitative findings. This creates a mix of quantitative and qualitative methods, making it a mixed-method research approach. Using quantitative research to look into the 'what' and have qualitative research to find out more about the 'how' (Brannen, 1992).

Qualitative aspect

An interpretive qualitative approach is used through interviews (Merriam & Tisdell, 2015). For this, semi-structured interviews with involved stakeholders that result data will be held, questioning them about the governance options and barriers to not implementing them. These interviews are exploratory with no testable hypothesis, to add to a more conceptual body of knowledge (Dicicco-Bloom & Crabtree, 2006). The novel focus of this IoT research is based on assumptions and uncertainties. A qualitative approach is more suited to explore different contexts within the research area (Fossey et al., 2002). Using guiding questions (see Appendix E: Interview protocol) as probes for an informed conversation, and to acquire the information about predefined themes (Qu & Dumay, 2011). The goal is not to generalize a specific finding to a larger population but *to "make logical generalizations to a theoretical understanding of a similar class of phenomena"* (Popay et al., 1998, p. 348).

Quantitative aspect

Quantitative analysis will be used on a dataset of Cybersprint consisting of 1649 IoT devices. Analysis of this dataset in combination with a vulnerability database (CVE) and WhoIS database will provide findings on the type of IoT devices, common vulnerabilities, and identification of stakeholders involved. It will also provide insights into what data is available and what can (or can not) be concluded from this data. This type of quantitative research is more suited for datasets and will give an insight into more generalizable conclusions (Napolitano, 2019). Using quantitative analysis on a dataset will be able to provide reproducible findings. The findings will therefore also be non-biased from the researcher's point of view. The results can be biased through a data bias, which will be addressed in chapter 5.

2.2. Research sub-questions

Within the general research method of mixed-method research there are specific research methods used to answer different sub-questions. The main research question will be answered by answering these sub-questions and using results as input for other sub-questions.

2.2.1. Sub-questions 1 & 2

Answering sub-question 1 forms the basis of this research by defining the core concepts and setting key characteristics. Answering sub-question 2 will provide a comparable basis for research but related to the governance capabilities and boundaries. The sub-questions are:

SQ1:*What are current relevant cybersecurity risks and principles in IoT devices described in literature?*
SQ2: *What principles from current governance applicable to IoT devices can be learned from literature?*

The method used to answer sub-question 1 and 2 is an academic literature review. First, IoT cybersecurity is explored and relevant IoT and security issues are characterized to answer research question 1. The next part will explore IoT governance and determine relevant factors to answer research question 2. The literature reviews form the background for the following research questions.
A selection of literature is made. The first selection is based on title and citations, and the following selection is based on reading the abstract. From this, the input for the literature reviews is around 15 academic papers per sub-question to ensure a well-backed literature review.

The output for sub-question 1 is an overview of the current academic literature concerning IoT and security, distilling literary findings relevant for this research into a summarized overview of IoT characteristics and IoT security characteristics to answer question 1.
The output for question 2 is an overview of relevant characteristics related to IoT governance found in the literature. Distilling relevant literary findings for this research into a summarized overview of governance aspects to find why current legislation works or does not work. These governance aspects and characteristics will be used as input for sub-question 5 and input for the synthesis in sub-question 7.

2.2.2. Sub-question 3

Using the literature studies in sub-question 1 and 2 as theoretical background, network scan data on IoT devices will form the empirical context of this research. The gathered network scan data is combined with the Common Vulnerabilities and Exposures (CVE) database to find security risks and the WhoIS database to find IP registrations. By analyzing this data, the following question will be answered:

SQ3: *What information in terms of devices and stakeholders can be found in the scan data of The Hague?*

To analyze the dataset, manual exploration needs to be done to uncover what information the dataset contains. This will consist of:
- *Categorizing IP addresses from the dataset* (finding IoT devices)
- *Classifying devices based on security vulnerabilities* (finding common vulnerable devices)
- *Looking for identifiable information* (device type, location, WhoIS registration)

Even though this is exploratory data exploration, the main expectation is the ability to (with certainty) identify device users (in combination with the CVE and WhoIS database) from IoT devices used in The Hague. From data exploration, it becomes evident that this expectation is not valid.

The disadvantage of this method is finding no relevant information from the dataset. By itself, this means no stakeholders or vulnerabilities can be identified. Within this research, this causes difficulty in designing governance options since there is less information available about the devices or stakeholders.

The input for answering this sub-question will be the entire dataset of 1649 IP addresses provided by Cybersprint. Information can be distilled from this data. After this manual exploration, the output will consist of findings from the dataset on different device types, device locations, and identifiable information found in the dataset. The findings on the IoT devices found in the dataset informs the research in terms of identified stakeholders and possible governance options. To answer that question, stakeholders need to be identified from the data. This will be done in sub-question 4.

2.2.3. Sub-question 4

From the initial analysis into the devices for sub-question 3, the next step will be to select the stakeholders that are or should be involved based on the network scan data and the literature review for sub-question 2. This will answer sub-question 4, being:

SQ4: *Who are the relevant stakeholders resulting from the IoT network scan data of The Hague and the literature?*

The analysis performed in sub-question 3 will form the contextual basis from which the most relevant actors will be selected. Next to this, any stakeholders that are not involved based on the data but result from the literature review in chapter 2 is selected.
The empirical ground for involving these actors will automatically be argued by finding the main identifiable stakeholders from the dataset. This will provide a starting point for the design of governance options based on the stakeholders identified. The disadvantage of this is the data bias resulting in stakeholders being excluded if they are not part of the dataset. The same disadvantage is the exclusion of stakeholders simply because they should be included but are not considered. To cope with this disadvantage, the stakeholders will be selected from the dataset and the literature.

The input to answer sub-question 4 will be the analyses performed in sub-question 2 and sub-question 3. The same IoT data will form the basis to identify the most relevant stakeholders that can already be found in the findings from sub-question 3. The output of this sub-question will be a selection of stakeholders to be used as input for sub-question 5. These stakeholders are the basis on which the next steps of research will focus.

2.2.4. Sub-question 5

Based on the identified stakeholders, an inventory can be made on the governance options available. By doing this, the following question will be answered:

SQ5: *What governance options are available to the identified stakeholders?*

For each stakeholder, a selection of governance options will be made that could be possible. The actual validation of these options is not the focus of this question. Different stages of an IoT device are used to assess the possible options during that stage structurally. The main goal is to find governance options for each stakeholder based on literature, personal communication, and brainstorming. The output will be a selection of different types of governance options based on the prevention, detection, and remediation of vulnerabilities for each stakeholder. The disadvantage is not being able to think of every possible governance option since that is impossible. The output will be types of governance options for each stakeholder that will be validated for the next sub-question.

2.2.5. Sub-question 6

The governance options defined in sub-question 5 will be validated through desk research and interviews with the defined stakeholders from sub-question 4. To answer sub-question 6:

SQ6: *How do the involved stakeholders view the identified governance options?*

The defined options of sub-question five will be validated to assess their feasibility. Using desk research will provide the ability to find out and compare the designed governance options with other governance options to find out why they work or not work. Interviews with the stakeholders identified in chapter 4 will give the possibility to use the governance options of question 5 as input and validate them, by highlighting the boundaries and conditions needed for implementation. The disadvantage is not being able to go through every possible governance option in complete detail; this is dealt wilt by using categories of governance options. The output of this question will be a selection of validated governance options and the boundaries/conditions for implementation to be used for the framework in sub-question 7.

2.2.6. Sub-question 7

Using a synthesis of information from the previous research questions, a conceptual framework will be made to answer the following research question:

SQ7: *How can these governance options be used to reduce the presence of vulnerable IoT devices?*

Using the identified stakeholders, the type of governance options, concepts from literature, and the conditions needed for these options to happen as input, a conceptual framework will be proposed. Through synthesis of the information provided to answer previous sub-questions it becomes clear what path can be taken towards implementing governance options to reduce IoT vulnerabilities. The disadvantage of such a framework is the inability to include every relevant concept from literature, therefore making this framework specifically designed for this research.

2.2.7. Main research question

Using the filled in conceptual framework as input, the main research question will be answered. The main research question is:

How can the municipality of The Hague use governance instruments to decrease cyber vulnerabilities in IoT devices?

Using the conceptual framework and information of sub-question seven as input, the outcome will be applied in a recommendation for the municipality of The Hague. Giving a conclusion about the central governance needed to address IoT vulnerabilities and the main obstacles to implementing this. The outcome for this question will be and advice and a discussion of the performed research.
An overview of all research steps and chapters can be found in figure 2.1.

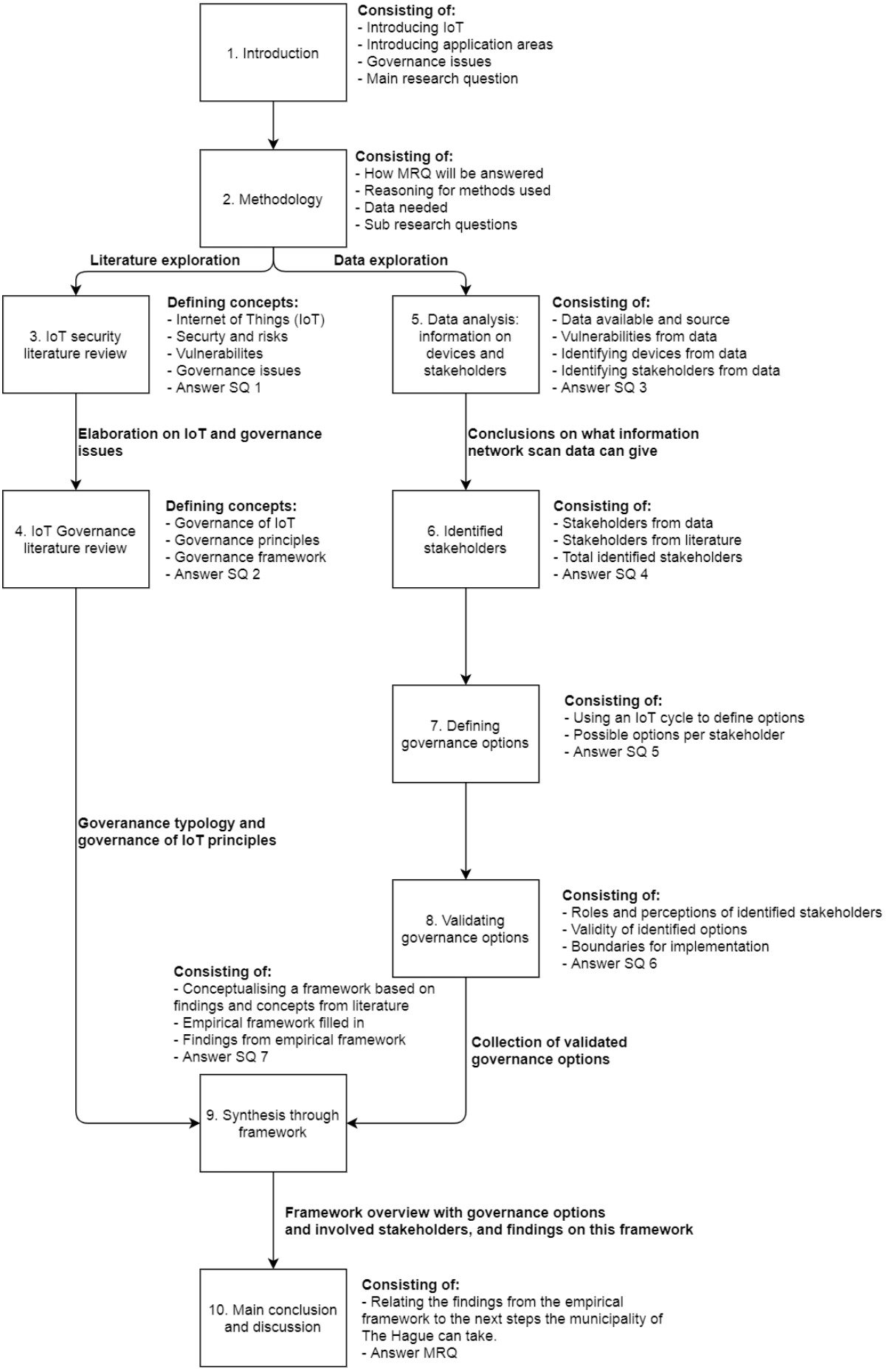

Figure 2.1 General overview of research flow and steps taken.

3 IoT and security in literature

This academic literature study will give a summary of relevant insights concerning IoT and security issues. This chapter is organized thematically, and first IoT characteristics will be defined, after which the aspects of IoT networks will be laid out through an IoT security architecture (Ning & Liu, 2012). By first dissecting IoT into layers, different concepts are defined, and possible vulnerabilities can be assessed. This will be done through smart city literature. Security issues will be looked into per IoT layer, giving essential background information for the following research chapters. From this specification of security issues per layer, a selection of security principles will be made. These principles form guiding when defining security solutions. By following this structure, this literature study will answer the question: What are current relevant cybersecurity risks and principles in IoT devices described in literature?

3.1. Literature search method

This literature study was conducted through the use of SCOPUS and Google Scholar as scientific databases. Google Scholar mainly was used for the first exploratory research, after which SCOPUS was used to find the most significant part of the literature. The keywords were variations of *(IoT OR internet of things) AND security*, and included *challenge*, *difficulty*, *metrics*, *measure*, *smart*, *community*, and *cities*. This was done to find the most relevant literature: defining IoT and security related to security issues.

3.1.1 Selection criteria

The selection criteria for literature to be relevant were through title and citations since a higher number of citations indicates scientific relevance (Aksnes et al., 2019). Recent (less cited) papers were also found, but their relevance between other (more cited) literature was difficult to determine and therefore left out. After an initial selection of papers based on title and citations, the selection encompassed roughly 40 papers. From reading the abstracts, the twelve most relevant papers when it comes to addressing security issues specified for IoT were selected. These selection steps ensured only highly cited papers with relevant content about IoT security would end up in this literature review. The papers from Wahab et al. (2017), Abdul-Ghani & Konstantas (2019) and Ning & Lui (2012) are the only exceptions and were selected through the references of other relevant literature *(snowballing)*. In table 3.1 an overview of selected papers.

Table 3.1 Giving an overview of selected papers and used relevant findings.

Authors	IoT analysis and architecture	Smart city application	Security issues	Security principles	Citations
Mahmoud et al., 2016	X		X	X	473
Hassija et al., 2019		X	X		256
Arasteh et al., 2016	X	X		X	287
Zhao & Ge, 2013	X		X		572
Frustaci et al., 2018	X		X	X	323
Gharaibeh et al., 2017	X		X		259
Zhang et al., 2017	X	X	X	X	335
Ammar et al., 2018			X		456
Bishop, 2003				X	2745
Wahab et al., 2017	X		X		33
Abdul-Ghani & Konstantas, 2019			X	X	32
Ning & Liu, 2012	X		X	X	167
Granjal et al., 2015				X	879
Hammi et al., 2018		X		X	135
Talari et al., 2017	X	X		X	295

3.2. Security architecture of IoT

To structurally assess the security of the Internet of Things seems like a difficult task considering the heterogeneous nature of a socio-technical system. Interconnecting physical devices from the real world in a network and combining information from different embedded sensors within these objects is the central concept of IoT (Wahab et al., 2017). Related to security is a growing attack surface created by the heterogeneous devices carrying security issues (Frustaci et al., 2018). Within the literature, a recurring approach is to analyze IoT according to a security architecture that divides IoT into three parts: a perception layer, network layer, and an application layer (Frustaci et al., 2018; Gharaibeh et al., 2017; Wahab et al., 2017; Zhao & Ge, 2013) (figure 3.1).

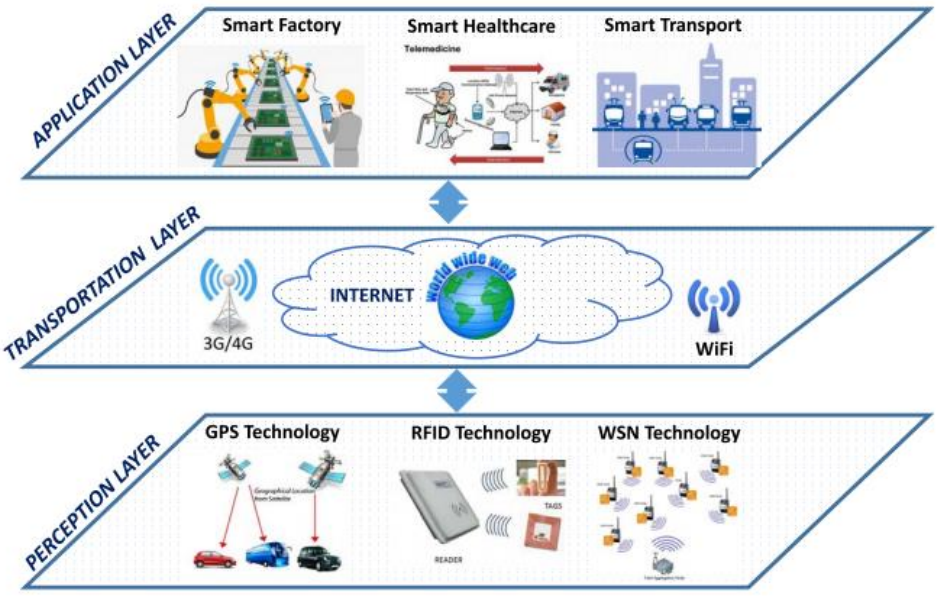

Figure 3.1. A conceptualization of the security architecture of IoT (Frustaci et al., 2018)

The IoT security architecture is created not to provide pure technical solutions to security problems but to analyze security issues in a broader context of the IoT system. As stated by Ning & Liu (2012, p. 1): *"IoT security issues are not a simple technically tough problem, but a multidimensional topic which combines the information security, network security, infrastructure security, and management security".* This indicates the complexity of the system. Therefore, the recurring security architecture (Ning & Liu, 2012) is used as the basis of analysis and will be used to apply IoT's different areas and security issues (see figure 3.2).

Application layer	→	Application service data security *(Smart cities, smart homes etc.)*
		Application support security *(cloud computing, analytical services etc.)*
Network layer	→	Network transmission and information security *(internet, mobile communication network)*
Perception layer	→	Perception layer local security *(RFID, sensors, Bluetooth, GPS etc.)*

Information security	**Physical security**	**Management security**

Figure 3.2. An overview of the architecture by Ning & Liu (2012) adapted by Zhao & Ge (2013)

These three layers can be related to the information, communication, and physical world (Zhang et al., 2017). There is a distinction to be made into the types of security concerning IoT. As used in the security architecture by Zhao & Ge (2013), there are three areas of security to keep in mind when looking into the layers of IoT (table 3.2).

Table 3.2 Three different areas of IoT security.

Information security	Relates to all user information and sensory information found on an IoT network. This information can be input from users, input from sensors, automatic data collection, or metadata from the network. Altogether this data needs to be protected for potential risk of exposure to malicious actors. Information can be seen as the commodity that uses the infrastructure of IoT devices and networks to come to the user through the application layer. Capturing, interpreting, and representing data through aggregation, protocols, and algorithms are part of information security (Ning & Liu, 2012).
Physical security	Relates to all security issues concerning the IoT devices themselves and the sensors involved. How physical devices and sensors, like environmental monitoring, motion detection, or recording and tracking, can be secured (Ning & Liu, 2012). Any compromise of an IoT device or sensor resulting from physical activity, like tampering with the device or sensor, or theft.
Management security	Relates to the heterogeneity of IoT networks and the issues in making variations of networks, sensors, and devices work together in a secure and manageable manner. By having different kinds of information sources (user input, sensor collection, and network information). This security aspect entails the application requirements and human interaction through regulations and standards (Ning & Liu, 2012).

Between these three security types there is an overlap. By compromising physical security, it could be possible to violate information security. By having inadequate information security, the management of IoT devices could be at risk: creating a more considerable management security risk. Classification of IoT in three different layers and relating it to three types of security provides structure to specify security issues per layer and security type.

3.3. Heterogeneity in IoT

Compatibility between devices, interoperability and network management creates security vulnerabilities due to network heterogeneity (Zhao & Ge, 2013). The increasing use of IoT requires communication standards suited for different types of 'things' (Hammi et al., 2018). Network protocols are targeted at homogeneous networks, making current security protocols unfit for application to IoT (Hammi et al., 2018; Mahmoud et al., 2016). A multitude of networks, interface designs, hardware, software and capabilities create a large surface area for security threats. System components are tightly connected to perform a task or service that requires integrated hardware and software. Combining this multitude of devoted services creates a challenge for smart cities and IoT, for which 'collaborating schemes' between stakeholders should be developed (Arasteh et al., 2016). This complexity increases the chance that an attack can occur on different IoT devices and make its way through different objects and application areas through this connectedness (Ning & Liu, 2012). The interconnectedness creates an opportunity for attackers to gather information from different sources (networked objects) to use in criminal activities (Mahmoud et al., 2016).

What is the risk for IoT?

Protecting the network is vital in the IoT, but safeguard the objects in the network is equally important. Things must have the ability to know the state of the network and the ability to protect themselves from any attacks against the network. Protocols within IoT objects and software that can respond and adapt security levels to changes in the network will cope with the heterogeneity (Mahmoud et al., 2016). Security solutions can focus on a single software or object, but due to heterogeneity, this becomes a challenge (Talari et al., 2017). There are many different devices in IoT with various vulnerabilities leading to the security issues to be addressed, and therefore no general solutions or fix applicable to all devices. With no easy way to fix these vulnerabilities, the most significant security challenge is a lack and inability of tailor-made solutions.
Another IoT issue that comes from this heterogeneity is the number of devices and the ability to keep track of every device to ensure security. From home IoT to city IoT, connecting networks requires management on different levels, which becomes an issue with heterogeneous networks and devices.

3.4. Smart cities

The evolving use of "*computation and communication resources"* to provide support and services adds value to the living conditions within a city (Hassija et al., 2019). This more general concept includes different smart subsystems that, when combined, form the smart city concept. As defined by Gharaibeh et al. (2017, p. 1): *"A smart city employs a combination of data collection, processing, and disseminating technologies in conjunction with networking and computing technologies and data security and privacy measures encouraging application innovation to promote the overall quality of life for its citizens and covering dimensions that include: utilities, health, transportation, entertainment and government services".* This also includes smart homes that use IoT devices to manage and control smart traffic control, smart environments with IoT sensors, smart business process management, etc. This shows the broad scope of the smart city aspect.

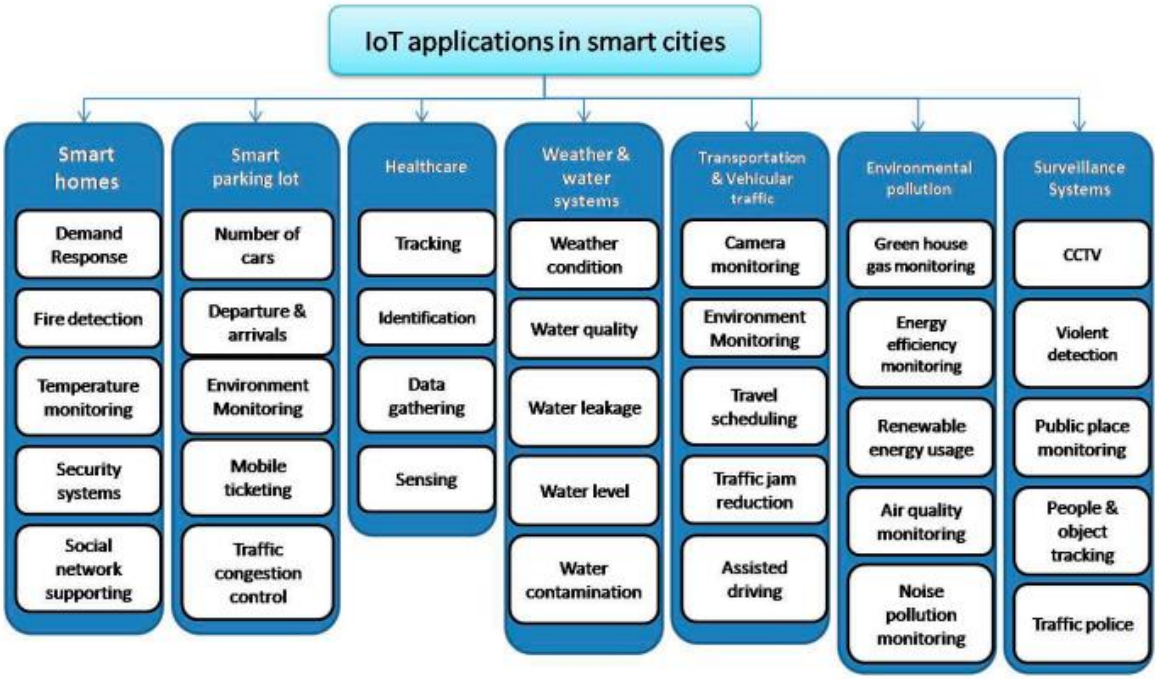

Figure 3.3. Example applications of IoT within a smart city (Talari et al., 2017)

The three aspects defined as smart city objectives are the cost of living, sustainable environment, and the quality of life (Gharaibeh et al., 2017). The use of IoT systems creates privacy issues for users (Hassija et al., 2019). Any use of a 'smart service' requires data to be collected, and this data collection creates a risk of exposing this data. For example, providing your location to an IoT service puts you at risk of leaking your location data. Using a webcam to monitor a public area puts this video stream at risk of being viewed by malicious actors. These aspects are given in an overview by Talari et al. (2017) (figure 3.3), emphasizing the communication aspect: the network of IoT devices that exchange data.

Table 3.3 An overview of smart city applications (Zhang et al., 2017) and categorization

Subsystem	Application	Leading actor	Goal
Smart energy	Smart energy	Private	Sustainable environment/cost of living
	Smart grid	Public	Quality of life/sustainable environment/cost of living
Smart living	Smart surveillance	Private	Quality of life
	Smart recycle	Private	Sustainable environment/quality of life
	Smart community	Private	Quality of life
	Social media	Private	Quality of life
	Smart home	Private	Quality of life/sustainable environment/cost of living
Smart services	Smart parking	Private/public	Quality of life
	Intelligent transportation	Private/public	Quality of life
	Intelligent healthcare	Private/public	Quality of life/cost of living
	Intelligent governance	Public	Quality of life
Smart environment	Smart weather	Private/public	Quality of life/sustainable environment
	Environment monitoring	Private/public	Quality of life/sustainable environment
Smart industry	Intelligent industry	Private	Cost of living
	Intelligent control	Private	Cost of living

It's apparent that the smart city concept encompasses many subsystems (see figure 3.4), and these rely on the usage of IoT in a public and private context (see table 3.3.). This heterogeneity of systems comprised of devices and sensors rely on the use of data. The quantity of heterogeneous data collected in a smart city requires standards for data gathering to ensure data acquisition and management (Gharaibeh et al., 2017). This is also where the security issues for the application, network, and perception layer come in. Conventional off-the-shelf security and privacy solutions cannot solve all security challenges of IoT networks within a smart city (Zhang et al., 2017). Security solutions seem to be specified on technical solutions, which seems unfit for use in smart cities that includes many different actors and creates a socio-technical system.

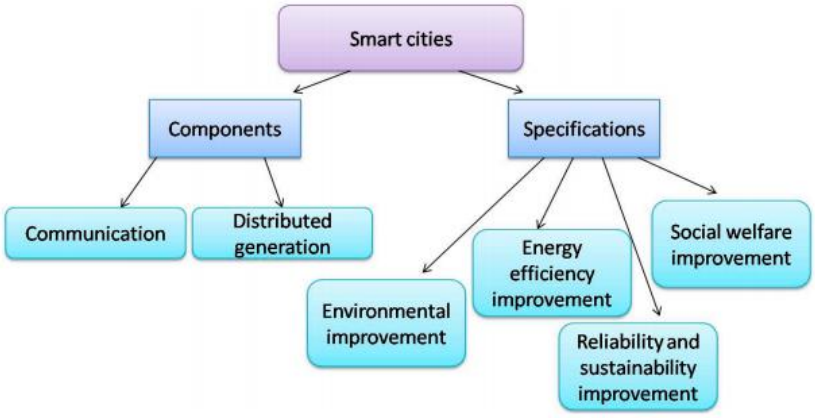

Figure 3.4 An overview of smart city specifications (Talari et al., 2017) and the components needed. Emphasizing a distributed network of devices that exchange data through communication.

3.5. Security issues

Security issues within IoT start at the device level. This only affects the users and could relate to vulnerabilities that risk their personal information. However, these 'small' vulnerabilities can be exploited and interfere with a network. By infecting a device in this way, the single user's risk can result in other users in the network being at risk and possibly the internet service provider. Therefore, looking at vulnerabilities and threats in different IoT layers creates an understanding of security issues that can result from the network scan data used in the following chapters.

3.5.1. Application layer

The application layer is also called software layer, and in some literature also includes a processing layer (Wahab et al., 2017). This layer consists of the added service through a smart environment presented to a user (Mahmoud et al., 2016). This is the layer of IoT that results from the perception and network layer being used to provide some IoT functionality to the user. This is also described as the 'data dissemination layer' (Gharaibeh et al., 2017). This *'service-oriented layer'* provides a service to the user (smart home, smart environment, smart transportation etc.) by processing the data from the perception and network layer and combining it with user data (Wahab et al., 2017). This user data can be a request for action, information, or general usage. Therefore, information security regarding confidentiality, integrity, and availability is most relevant for this layer (Mahmoud et al., 2016). Through a web interface run by the IoT device, different services are used with additional data and authentication mechanisms. Integration of these applications has to ensure data privacy and identification, which is difficult (Mahmoud et al., 2016).

Potential security issues on this layer through the service provided (mostly through a web interface belonging to the device) are:
Unauthorized Access *(Wahab et al., 2017):* Data storage is found within the application layer. By acquiring unauthorized access in the application layer, data can be stolen or deleted, resulting in malfunctioning of the network.
Malicious Insider *(Wahab et al., 2017):* When an actor within an IoT network (with access to the network) becomes a malicious actor and starts collecting sensitive information and attacking the network.
Application security *(Wahab et al., 2017):* By using the application of IoT as a web service, any attackers can connect to the internet and attempt to steal sensitive information being used in the application.
Data security *(Wahab et al., 2017):* The application service provider (mainly manufacturers) needs to ensure data security and backups. Data theft can occur with insecure storage or backup practices.
Underlying infrastructure security *(Wahab et al., 2017):* When using the application of an IoT service provider (primarily manufacturer as well), the underlying security and technology layers are not accessible. Meaning security risks in these layers can cause vulnerabilities.
Phishing Attack *(Wahab et al., 2017):* Overlap with a social engineering attack. A malicious actor can gather sensitive information by having users log in or authorize themselves on a fake online environment.
Virus, Worms, Trojan Horse and Spyware *(Wahab et al., 2017):* Using malicious software (malware) to infect a network or system and gathering confidential information. This to disrupting the network or acquire access to the network.
Malicious Scripts *(Wahab et al., 2017):* When services run through the internet, a complete system shutdown can occur when running a malicious script that triggers such a shutdown. This can be sent to the network. By injecting a malicious script into a web service that the user uses, the IoT information of the user can be taken and used to take down the entire IoT system (Hassija et al., 2019).
Denial of Service *(Mahmoud et al., 2016; Wahab et al., 2017):* Stopping a user from using the network or resources by sending an overload of information to this network. This will make the objects within the network unable to handle all information, including requests by the user to provide a service.
Data Protection and Recovery *(Wahab et al., 2017):* Inadequate handling by procedures or data processing, users' privacy can be violated and put at risk.

These threats can be categorized into three overlapping categories: data leakage, denial of service, or an injection of malicious code (Frustaci et al., 2018). The application layer directly involves the users of IoT. That means because of the variety of applications and heterogeneous aspects of IoT, the types of users and required data will have to be kept in mind for application. On this layer, users should know what data is used,

how, by whom, and having the ability to change the amount of data shared with the application or service (Mahmoud et al., 2016). An overview can be found in table 3.4.

Table 3.4 Examples of security threats, categories, and security type on the application layer.

Type of threat	**Categorized attack**	**Type of security**
Unauthorized Access	Data leakage	Information security
Malicious Insider	Data leakage/denial of service	Information/management security
Application security	Data leakage	Information security
Data security	Data leakage	Information security
Underlying infrastructure security	Data leakage/denial of service	Information/management security
Phishing Attack	Data leakage	Information security
Virus, Worms, Trojan Horse and Spyware	Injection of malicious code	Information security
Malicious Scripts	Injection of malicious code/denial of service	Information/management security
Denial of Service	Denial of service	Management security
Data Protection and Recovery	Data leakage	Information security

Remediation efforts to prevent or decrease the described security issues can be divided into technical and non-technical solutions (Zhao & Ge, 2013). Technical solutions mostly concern authentication, certification, and safe exchange of security keys through cryptography (related to security-by-design) (DCMS, 2018). This also includes protecting personal information through technical measures. How these technical solutions work or function will not be in the scope of this research, but the actors and governance involved to implement these technical solutions will be relevant. This technical governance mostly concern security and governance by design, through manufacturing.

Non-technical security solutions at the application layer involve human and technology interaction and are generally aimed at safe security practices to ensure the described threats can not occur. This includes increasing user awareness in terms of safety. Knowing how to use an IoT device safely and having more knowledge about sharing and using confidential information will decrease security threats (Zhao & Ge, 2013). This awareness includes *"resource management, physical security information management, password management, etc."* (Zhao & Ge, 2013). The role of users is indispensable to prevent attacks by changing default passwords, for instance (Abdul-Ghani & Konstantas, 2019).

What are the risks for IoT?

Considering IoT focuses on consumers and users that require services, the application layer is the communication layer for this service. Current issues on this layer come from misconfigurations that result in the security threats described, which relates to having a safe service/application to access the service, changing default passwords, general security practices like keeping credentials safe, and security attitudes by users. Through a lack of these basic security controls, vulnerabilities in the application layer result in security risks for users, with the possibilities of escalating threats for the whole network. This makes a secure device as safe as the user's security practices. This could indicate a possible common interest between users using a device safe and manufacturers making a device safe. These issues could be solved through individual responsibilities, initialised by this common interest. This will addressed further in chapter 6: stakeholder identification.

3.5.2. Network layer

The communicating layer between the perception layer and the application layer also called the 'data-processing layer' (Gharaibeh et al., 2017). The task of this layer is to exchange and analyze data from the perception layer to distribute it to the right network for application (Ning & Liu, 2012). This layer connects physical devices and networks through specified protocols (Wahab et al., 2017). Routing and transmission of these data networks, as well as mediating between sensory information and the application area of IoT (Mahmoud et al., 2016)

Potential security issues in this layer that result from gaining access to a network as an outsider are:

Traffic analysis attack *(Mahmoud et al., 2016; Wahab et al., 2017):* Common attack that first inspects a network (using port scanners, for instance) to acquire information on the network. Through the use of a web browser, confidential information from connected devices can be obtained.
Malicious Code Injection *(Wahab et al., 2017):* Injecting malicious code into a network causing the network to malfunction or shut down.
Sleep Deprivation Attack *(Wahab et al., 2017; Zhao & Ge, 2013; Mahmoud et al., 2016):* Tampering with the 'on' time of device through the network, and by keeping a device running draining the batteries of such sensor or object ensuring an unusable device (temporarily) and disrupting the network.
Sinkhole Attack *(Wahab et al., 2017):* Creating and sinkhole and attract or reroute all traffic within a network to this sinkhole. Acquiring confidential information and disrupting traffic in this network.
Man in the Middle Attack: Infiltrate in the communication between one node to other nodes, and acquire sensitive data. This can mean getting complete control over the data between sender and receiver without any of them knowing (Hassija et al., 2019)
Routing Information Attack *(Wahab et al., 2017):* Changing a network's routing by creating loops and sending out false information. This malfunctions the network.
Wormhole attack *(Wahab et al., 2017):* Linking the original location in a network with a new location creates a so-called 'wormhole' that sends information to another location.
Denial of Service *(Mahmoud et al., 2016; Wahab et al., 2017):* Stopping a user from using the network or resources by sending an overload of information to this network. This will make the objects within the network unable to handle all information, including requests by the user to provide a service.
Hello flood attack *(Wahab et al., 2017):* Sending out many 'useless' information in a network, creating a block of the information channels in a network, blocking the entire network in the process. Comparable to traffic and traffic jams. Depleting resources by sending information and request to a service (Hassija et al., 2019).

These threats can be categorized into the overlapping categories of routing attacks, denial of service attacks, and data transit attacks (stealing data) (Frustaci et al., 2018). An overview of this can be seen in table 3.5.

Table 3.5 Examples of security threats, categories, and security type on the network layer.

Type of threat	**Categorized attack**	**Type of security**
Traffic analysis attack	Data transit	Information security
Malicious Code Injection	Denial of service	Management security
Sleep Deprivation attack	Denial of service	Physical security
Sinkhole attack	Routing/denial of service	Management security
Man In The Middle attack	Data transit	Information security
Routing Information attack	Routing/denial of service	Management security
Wormhole attack	Routing attack	Information security
Denial of service attack	Denial of service	Management security
Hello flood attack	Denial of service	Management security

What are the risks for IoT?

IoT uses 'traditional' network technology, and this older network routing is not suited for IoT use. This is due to the *"node arrangement random, autonomic, unreliability of energy limitation and communication, and dynamic topology"* (Zhao & Ge, 2013). This causes risks in primarily management and information security. It creates the situation where multiple stakeholders are involved with an IoT network and use network infrastructure not adapted to IoT. This goes back to the heterogeneity issue of IoT: too many different devices and networks to manage, causing too many different vulnerabilities to solve.
To remediate these network security issues and ensure an available network capable of handling the vast amounts of data required, the technical solutions would be the use of different authentication and key exchanging mechanisms, as well as identity verification (Zhao & Ge, 2013). Using encryption and authentication to create more trust between involved actors in a network (Zhang et al., 2017). The social aspect of this entails having policies in place to ensure the availability and integrity of the data; in the process keeping the data confidential and privacy-sensitive information out of reach from unauthorized actors.

3.5.3. Perception layer

Also called the 'physical layer' within the literature and the 'data acquisition layer' (Gharaibeh et al., 2017). It consists of real-world physical devices and sensors that provide information from the physical environment. These devices are responsible for information gathering and transmission to the network and application layer (Wahab et al., 2017). The main issue in this layer is that sensors and small IoT devices, in general, have high heterogeneity and low processing power. This makes it almost impossible to create a complex security solution (Zhao & Ge, 2013).

The perception layer's potential security risks and issues are mostly related to physical security, which then transfers to information security or management security. A selection of these security issues are:

Sensor interference *(Mahmoud et al., 2016; Wahab et al., 2017):* Blocking signals to stop IoT sensors from working. This could be wireless sensors through network interference or physical tampering with devices or sensors to change the workings of such objects.
Physical damages *(Mahmoud et al., 2016; Wahab et al., 2017):* By damaging or tampering with the IoT system or components, a network can be made (temporarily) unusable.
Social engineering *(Wahab et al., 2017)***:** Through exploiting the user to acquire sensitive information. This can be done by physically communicating with the IoT network or with the user itself. For instance, misleading the user into giving away valuable information by physically taking another identity or contacting the user on behalf of another actor to acquire valuable information. Through this relatively easy method, large amounts of private information can be obtained from a victim (Zhao & Ge, 2013).
Acquiring access to information through tags *(Wahab et al., 2017):* Due to a lack of proper device authentication, a malicious actor can acquire access to tags of a device and modify, copy or delete data from it. It is then also possible to copy a tag, making the UUID not 'unique' anymore and creating uncertainty about the actual device's ID in the network.
Eavesdropping *(Mahmoud et al., 2016; Wahab et al., 2017):* Infiltrating a network or 'physically' looking into the connection between users and a device or vice versa to acquire sensitive information.
Spoofing *(Wahab et al., 2017):* Acting as a node in the IoT network and spreading information to acquire access to the entire network.
Node Capture *(Mahmoud et al., 2016; Zhao & Ge, 2013):* When a malicious actor controls an essential object in a network, the entire network's security is compromised.
SCA (Side-Channel Attack) *(Zhao & Ge, 2013):* By attacking devices, the side channels of these devices give out information on time consumption, power consumption, or electromagnetic radiation. This can be valuable information.
Selling of device with fixed key *(Ammar et al., 2018):* IoT devices might be encrypted or protected with a security key. This is secure unless the key can not be changed after deployment or use. This means a device that changes owner or gets sold will be vulnerable since the previous owner knows the security key.

These threats can be categorized into the overlapping categories of physical attacks, impersonation, denial of service, data transit attacks, and routing attacks (Frustaci et al., 2018). An overview of this can be seen in table 3.6.

Table 3.6 Examples of security threats, categories, and security type on the perception layer.

Type of threat	**Categorized attack**	**Type of security**
Sensor interference	Physical	Physical security
Physical damages	Physical	Physical security
Social engineering	Impersonation	Information security
Acquiring access to information through tags	Impersonation	Information security
Eavesdropping	Data transit	Information/management security
Spoofing	Impersonation	Information security
Node capture	Routing	Management security
SCA (Side-Channel Attack	Data transit	Information security
Selling of device with a fixed key	Physical	Information security

What are the risks for IoT?

The overall solutions to these issues are a secure software design to ensure management and information security (Zhao & Ge, 2013). For smart city applications, Hammi et al. (2018) adds that physical security is often compromised. Safe hardware configuration and security should ensure tampering is impossible (Wahab et al., 2017; Zhao & Ge, 2013). Adding adequate device authentication to ensure no 'tag cloning' can be performed as well as spoofing (Mahmoud et al., 2016; Zhao & Ge, 2013). Point-to-point or end-to-end encryption to devices will also remediate part of the security issues (Mahmoud et al., 2016). These solutions seem to lie at the manufacturer of such an IoT device, and therefore security-by-design. However, the issue with most IoT devices is the lack of physical computing power, meaning the devices are not even capable of the security measures suggested. Social engineering can be remediated by ensuring data privacy and protection from the user side, increasing security awareness (Mahmoud et al., 2016; Zhao & Ge, 2013) and ensuring users know how to identify malicious interactions and not share sensitive information data. This same approach has also been described as security measure for the application layer.

3.6. Security principles

Based on the described security issues, general security principles can be used to assess vulnerabilities. These are also found in traditional IT; however, the difference between IoT and traditional IT is openness: tweaking and adding hardware or software to a regular computer. IoT is closed, meaning that a device is final in terms of hardware and capabilities after it has been manufactured (Frustaci et al., 2018), also indicating "secure by design" instead of "add-on security" in conventional IT.

The lightweight hardware of IoT means that the resources to add elaborate security measures do not have much computing power or capabilities (Frustaci et al., 2018). Hammi et al. (2018) call IoT *limited to possess security protocols.* For IoT vulnerabilities to be exploited, the device's network has to be detectable by a malicious actor. This relates to security awareness among users (Mahmoud et al., 2016), indicating that some IoT devices are publicly accessible without the user knowing this: creating a security risk.
These security issues are emphasized by the lack of standards specifically designed for devices with limited resources and heterogeneous technologies; this minimal security makes IoT more vulnerable than conventional IT systems (Frustaci et al., 2018). These many vulnerabilities represent a fertile ground for already existing cyber threats. (Frustaci et al., 2018, p.1)

IoT creates novel challenges, but the security aspects of traditional IT systems also apply to IoT networks (Ning & Liu, 2012). Therefore the core of IoT security in literature uses the CIA triad or security triad (Abdul-Ghani & Konstantas, 2019; Granjal et al., 2015). (see figure 3.5).

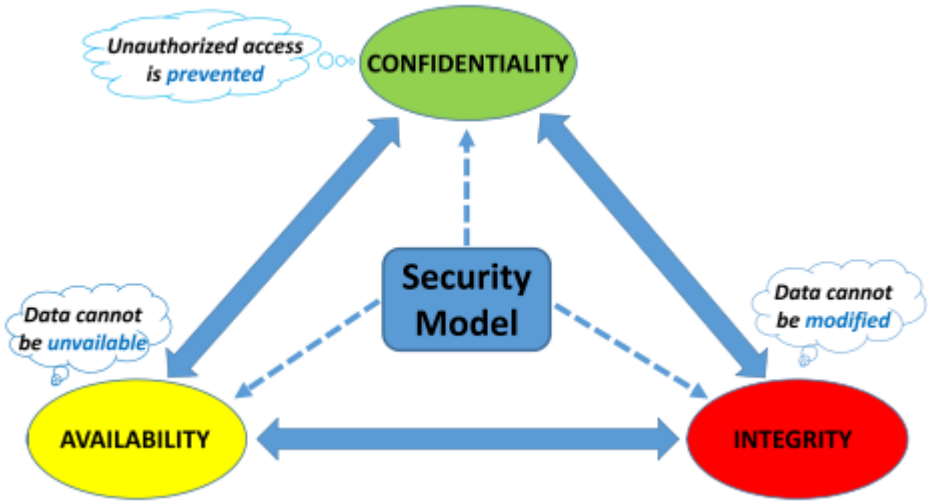

Figure 3.5 The security triad (Frustaci et al., 2018)

Based on the literature, these principles form the core of any system's security. This security triad also defines the core security issues of IoT in smart cities (Hammi et al., 2018). To define security principles for IoT added to this security triad will be privacy, usability, and policies.

Confidentiality

Confidentiality within information systems entails that data should only be available to authorized users, encompassing human, machines and services, and internal or external devices of the network (Mahmoud et al., 2016). Ensuring authorized users can access private or sensitive data (Frustaci et al., 2018). This overlaps with data management: users should be informed about how their data is managed and protected throughout usage (Mahmoud et al., 2016). This principle is a guiding principle in the security of information systems (Frustaci et al., 2018), primarily through access control or encryption. Confidentiality ensures authorized disclosure of data (Ning & Liu, 2012).

Integrity

Integrity relates to being able to confirm accurate data exchanges. If an object in the network sends information, knowing the information is correct and not interfered with, and having the 'right sender' (Mahmoud et al., 2016). A stakeholder would preferably erase data than having unauthorized people being able to view this data. (Bishop, 2003, p. 1). Integrity ensures accuracy and correct data (Ning & Liu, 2012).
To have data protected from external interference and ensure no data can be altered through data transit (Frustaci et al., 2018). The security aspect of non-repudiation is part of integrity: to ensure data validity is accepted by sender and receiver (Granjal et al., 2015; Zhang et al., 2017). This can also be done through building in proof that show what party handled the data to make denial about the use of the data unlikely, increasing integrity (Ning & Liu, 2012). Integrity, therefore, is about trust between parties, and proof of this trust. Implementing end-to-end security in IoT networks would safeguard integrity, however due to the lightweight nature of IoT sensors and devices integrity at 'endpoints' can not be ensured (Mahmoud et al., 2016)

Availability

The availability principle within IoT consists of two aspects. The first aspect concerns the use of data: The interconnected nature of IoT for smart purposes entails users should be able to use IoT services (and therefore have the correct data available) upon immediate request (Mahmoud et al., 2016). This is based on access of an accepted actor to view or use information or resources at any moment in any condition (Frustaci et al., 2018), which is usually the target principle of denial of service attacks. The second aspect involves services and devices: these must be available when a user wants to use these (Mahmoud et al., 2016). The IoT user intends to use the service for which the IoT device is designed and has no use for only the IoT device's data for this service. There must be no denial of authorized access to a network (Ning & Liu, 2012). The principle of availability also brings up the issue of privacy. To facilitate available data and IoT services, all required sensors and devices have to be connected to the internet constantly (Arasteh et al., 2016), and this increases security risks.

Added to these three general security principles of information systems, three more principles are added to define what 'good' security entails concerning IoT. These principles are chosen to specifically be valuable to the usage of IoT since they reoccurred as being important in other literature.

Privacy

The central aspect that returns in every other security principle is (the preserving of) privacy. It is primarily named in parallel to security (Gharaibeh et al., 2017), meaning privacy is so important it is not categorized within security itself. Privacy encompasses a broad scope of concepts that relate to privacy being respected or violated. Confidentiality, integrity, availability, access controls, and usability, for instance, all relate to privacy-induced security issues (Zhang et al., 2017). This is the granular scale of information collection, based on the heterogeneous devices and uses within an IoT system. Privacy as broad protection entails protection of: *"Any sensitive information (…) that may be derived from the observation of network activities."* (Ning & Liu, 2012, p. 4). This could include specific information like name, address, date of birth, online credentials etc., but also derived information like inferring when someone is at home through energy usage. All this sensitive information IoT devices and sensors collect have the ability to influence people's lives, and therefore, the privacy aspect comes back in every data collection or processing aspect of IoT (Zhang et al., 2017). That is also the main difficulty in privacy-related issues for IoT: usage of IoT is embedded in other tasks and routines through which sensitive information is gathered (Frustaci et al., 2018). Security mechanisms should protect the privacy of smart device users at all times (Arasteh et al., 2016). This is still an area to be researched more (Talari et al., 2017). The main overarching legislation that ensures privacy is not violated in terms of data collecting and management that IoT devices do, is the General Data Protection Regulation (GDPR). It has privacy principles overlapping with the described security principles (transparency, data minimization, accuracy, storage and collection limits, integrity and confidentiality) (Principles Relating to Processing of Personal Data, 2016). The GDPR will be addressed in chapter 4.

Policies and standards

The lack of policies and standards constitutes security issues. Due to the vast amounts of data gathered by IoT devices, only the information must be collected that is needed for the device or service to function. Most IoT devices do not have a user interface, and if they do it mostly does not provide a user with sufficient tools to view the data gathered and needed (Frustaci et al., 2018). By enforcing standards or policies that require this, privacy issues do not even have to become an issue by giving users information about their information. For instance for smart cities, where having no standards is a general issue (Hammi et al., 2018). IoT will affect society (security, transportation, personal devices, public spaces etc.), and policy will not only have to be developed for this, but IoT can also be used to develop policy decisions, from saving energy, monitoring pollution, or making decisions based on available data from IoT (Arasteh et al., 2016). This means policies will not only be used to create IoT security, but IoT security aspects can also be used by authorities to develop guidelines. This will also bring legal and social issues by making policies and enforcing them (Talari et al., 2017). Stakeholders in IoT that do not comply with regulations or standards can only be adjusted through legal action or disciplinary measure (Ning & Liu, 2012). Therefore security goals in IoT need to be incorporated in legislation and monitored. Standardized IP-based innovations form the basis to develop new IoT technologies (Granjal et al., 2015), so it is essential to have a solid policy foundation for development.

To conclude, when looking at security in IoT whether that be technical solutions or through governance options, policies and standards have to be kept in mind. Applying security principles to standards or regulations requires local regulation that will give the option to design, implement, and maintain the local IoT networks with the local practices in mind (Ning & Liu, 2012). Through local policies, 'effective and cost-efficient municipal services' can be realized (Hammi et al., 2018).

Usability

An aspect that mostly goes unnoticed is the usability of an IoT device, a broad concept. Considering the security principles discussed, usability for a device user will have to be taken into account for every issue related to IoT. Imagine a device that is produced and is used with all security principles in mind (confidentiality, integrity, availability, privacy, policies and standards). In this scenario, it is possible that, because of the security principles needed to function 'safe', the actual use of the device has disappeared. For instance, a smart speaker that is unable to access Spotify because of privacy regulations: making the device safe in terms of privacy but unusable in terms of intended purpose; or a webcam that is so 'secure' that accessing videos from it or using it requires so many steps that users will find a workaround by using an unsecured device. This means that 'intended use' must not be undermined by principles intended to make a device safer and not better.

3.7. Conclusion

Through this literature review, IoT was conceptualized through an overview of layers: the application, network, and perception layer. Through the example of smart city applications, the heterogeneous nature of IoT became evident. The different security issues involved relate to the three layers and types of security: information, management, and physical security.

The security risks described for IoT devices result from the heterogeneity of IoT services, devices and networks. The devices on the market use different hardware, software, protocols, and other technologies, which causes described security risks on the layers. This makes for a lack of generic security solutions since managing many different devices requires tailor-made solutions for specific devices or vulnerabilities.
Security issues on the application layer result from misconfigurations like secure access control to an IoT service set up by the manufacturer. However, the challenges for security issues on the application layer are security practices by users, like keeping credentials safe or changing passwords and keeping them safe. A lack of basic security controls from manufacturers and basic security practices from users on this layer creates vulnerabilities for individual users, possibly affecting a whole network.

For issues on the network layer, the heterogeneity of IoT devices again causes management issues. Too many different services and devices, using different standards and networks to manage. When too many devices with different network standards have to connect to the same network, the various vulnerabilities can not be solved with a generic solution.
IoT devices' perception or physical layer should be made ‘tamper free’, but this is a difficult task in practice. Secure software and hardware lie at the manufacturer and come from security-by-design. The lack of physical computing power in IoT devices create the issue of making suggested software security measures impossible.

Resulting from this is a selection of security principles (table 3.7). The key takeaway is an overlap between the described security issues and principles. Different security vulnerabilities can be used as backdoors to exploit the device or deploy other security risks. The resulting types of security and related principles that can be used to assess IoT vulnerabilities are shown in table 3.7.
This literature review forms the background information for the follow-up research questions. The sub-question is answered: What are current relevant cyber security risks and principles in IoT devices described in literature? The types of security and principles are related to the security issues found in the dataset in chapter 5. The next step will be looking into the governance needed to solve these issues, which will be discussed in chapter 2.

Table 3.7 Overall concepts from literature to assess IoT vulnerabilities.

Security layer	**Type of security**	**Security principles**	
Application, Network, Perception	Information, Management, Physical	Confidentiality	Ensures the ‘right’ actor can access the data used in IoT. Securing no data confidential data can be viewed by unauthorized actors.
		Integrity	Ensures the sender and the receiver trust data exchanges between IoT devices. With certainty, no data tampering or sharing with third parties were involved.
		Availability	Ensuring the IoT service and data needed for this application can be used and is available at all required times.
		Privacy	Ensuring confidential data collection is minimized, purposeful, lawful, and is not unknowingly gathered and shared with other parties. Consent and control of data ensure privacy is respected.
		Policies	Ensuring standardization, similarity, and policies to enforce IoT security will provide better security management and control.
		Usability	Ensuring that, with all security remediation measures in mind, the IoT or device is still usable for its intended purpose.

4 IoT and Governance in literature

This academic literature study will go through governance specified for IoT and the issues involved. Chapter 3 highlighted different IoT risks caused by device manufacturers or user practices, which come to light by the heterogeneous nature of IoT. By thematically going through defining governance and looking into the current focus of IoT governance literature, underlying governance principles will be described. By following this structure, this literature study will answer the sub research question: What principles from current governance applicable to IoT devices can be learned from literature?

4.1. Literature search method

This literature study was conducted through the use of SCOPUS and Google Scholar as scientific databases. Google Scholar mainly was used for the first exploratory research, after which SCOPUS was used to find the most significant part of the literature. The keywords were variations of *governance + (IoT OR 'Internet of things')* and keywords like *challenges, issues, security, stakeholders*, and *IoT*. Through this most relevant literature was found.

4.1.1. Selection criteria

The selection criteria for literature to be relevant was through the number of citations as defining criteria. First, an initial selection of papers was made based on the title and highest number of citations since a higher amount of citations could indicate more scientific relevance (Aksnes et al., 2019). This selection encompassed roughly 38 papers. The most relevant papers based on IoT and governance specification were selected from reading the abstracts or parts of the paper. This resulted in 15 papers. The papers of Jayawardane et al. (2015) and Brass & Sowell (2020) were found to contain relevant aspects in terms of IoT governance, and even though cited a relatively low number of times were therefore still included. The papers of Cetin, Ganan, Altena, Kasama, et al. (2019) and Cetin, Ganan, Altena, Tajalizadehkhoob, et al., (2019) resulted from the initial literature used to write the knowledge gap of this research, and were found to be relevant. In table 4.1 an overview of selected papers.

Table 4.1 An overview of the selected literature and aspects within this literature review.

Author	**Specification of governance**	**IoT specific governance**	**Highlights issues with governance**	**Governance principles**	**Citations**
Weber, 2013	X	X	X	X	97
Roscia et al., 2013					82
Weber, 2009		X	X	X	193
Perera et al., 2014			X		983
Abdul-Ghani & Konstantas, 2019		X	X		32
Borrás & Edler, 2020	X	X			24
Borrás & Edler, 2014	X				29
Jayawardane et al., 2015	X		X	X	9
Apthorpe et al., 2017			X		204
Zheng et al., 2018		X	X		118
Dutton, 2014		X	X		137
Roman et al., 2011		X	X	X	798
Wachter, 2018			X	X	28
Brass & Sowell, 2020	X	X	X	X	3
Kuerbis & Badiei, 2017	X				17
Cetin, Ganan, Altena, Kasama, et al. (2019)		X	X		18
Cetin, Ganan, Altena, Tajalizadehkhoob, et al. (2019)		X	X		5

4.2. IoT governance specification

The scope for governance will be any IoT devices that carry (unknown) vulnerabilities. Managing such IoT vulnerabilities requires *"pre-existing knowledge of IoT device design as well as knowledge of how these devices are deployed and behave within the Internet infrastructure, upon which they fundamentally rely for connectivity and "smart" functionality*" (Brass & Sowell, 2020, p. 1). Considering how devices are deployed and behave relates to governance, what can generally be defined as: *"policy-driven control over resources, systems and services"* (van Eeten, 2017, p. 446).

Innovations in IoT might stagnate because of organisational, institutional and public policy constraints (Dutton, 2014). The design of effective governance has to balance innovation and the protection of human rights (Roman et al., 2011). In that sense, governance is a comprehensive concept, but within governance, Borrás & Edler (2014) use *'governance of change',* consisting of public and private actors working together to change a socio-technical system. This applies to the governance of IoT. What drives this change in a socio-technical system is influenced by the interplay between institutions within a system and knowledge and innovations (Borrás & Edler, 2014, p. 24). To collectively create governance, different complex public-private partnerships will have to be realised. To conceptualise governance of change, the three pillars of figure 4.1 will be used. These three pillars of governance defined form the basic outline aspects that form governance. Essentially a who, how, and why.

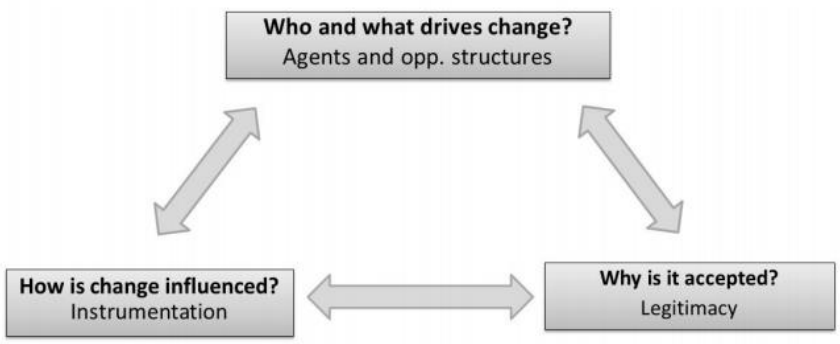

Figure 4.1 The three pillars of governance of change (Borrás & Edler, 2014)

Instrumentation

Concerning the 'how' question (how can governance be used), governance instruments are used as instrumentation. Governance instruments are defined as the tools to create public-private interactions and form social actions that different actors set to ensure some goal is reached: making the interplay between the institutional and technology side in socio-technical systems explicit (Borrás & Edler, 2014). There needs to be a balance between technological risks and regulations while also safeguarding innovations (Brass & Sowell, 2020).

For defining governance instruments, you must specify who will create the instrument, what it entails, and how these instruments will be implemented (Borrás & Edler, 2014). As set in chapter 1: governance instruments consist of public and privately led instruments, and these policy instruments and social agents' instruments and if these co-exist, they need to be coordinated together to ensure the governance goal is reached (Borrás & Edler, 2014). However, governance can be seen as *a double-edged sword* that creates structure and secureness in decision-making while also creating the ability to facilitate legitimacy in monitoring and controlling the system governance is designed for (Roman et al., 2011).

Legitimacy

Since governance is centred on collective coordination within society, there should be support for governance instruments. Therefore legitimacy is another aspect of the governance of change to ensure effective governance is supported by the stakeholders involved. Legitimacy means the involved stakeholders are represented and able to participate in the forming of governance and therefore create support for the input and output of the governance (Borrás & Edler, 2014). This is similar to representation, meaning that the

subjects of the governance (users and the private stakeholders) should be involved in forming governance decision (Brass & Sowell, 2020).

Smart cities

When it comes to defining governance for use in smart cities (and therefore IoT), Borrás & Edler (2020) specify this as *heterarchical, non-dominated* and *driven by state actors.* Meaning that no stakeholder is in charge within a hierarchy, and no stakeholder has a dominant say in how the socio-technical system should be governed. Therefore it's named as the 'primus inter pares' governance mode, in which the government takes the role of facilitator, promoter, and initiator of projects by using solutions provided by private actors and using tax money to (co)finance these solutions in a smart city (Borrás & Edler, 2020). This does not exclude the option of also having a government as the lead user. These are primarily local governments that drive smart city initiatives and have a say in implementation. It is mainly municipalities that own the infrastructure on which a smart city is developed. This means that for governance to be efficient, there should be access control by the involved stakeholders (Borrás & Edler, 2020).

When it comes to governance instruments used to establish smart cities, the main instrument at the moment can be seen as the use of narratives: by establishing an idea on how the future of a city should look like and involving stakeholders to be part of that change and get them more actively involved to set this idea (Borrás & Edler, 2020). This leads to the creation of public-private partnerships, procurement, legislation, contracts and rules, etc. The involved stakeholder supports all in light of the 'future idea' of the smart city for public services.

Multistakeholderism

Cyber governance is characterised by a decentral, multi-stakeholder aspect (Jayawardane et al., 2015). This multi-stakeholder aspect entails that different (groups) of actors are involved somehow, with some demands or values that need to be considered. Multistakeholderism is described as the next step in governance to include society (Weber, 2009). This does not mean equal involvements of all actors, but a more thought out governance structure that considers all involved actors. This requires cooperative effort (Roman et al., 2011). An important question is first to define who could be a legitimate stakeholder (Weber, 2009)—described as the "*balance of powers between private industry, international technical governance institutions, governments and civil society"* (Jayawardane et al., 2015, p. 5). For instance, it states that at the moment only control the norms and (international) rules. The private sector is the developing actor that has to comply with these rules, and therefore the technical aspect is designed and operated by the private industry. This hinders transparency and accountability since, as long as private actors comply with the (limited) rules concerning cyber space, they can develop any IoT technology they want.

Keeping multistakholderism in mind will affect by creating an equal playing field. Single actors should be unable to control the whole cyberspace, and the stakeholders most suited to deal with certain situations or data should be the ones in charge of that aspect (Jayawardane et al., 2015).

Challenging aspects that undermine effectiveness and legitimacy are described by Jayawardane et al. (2015). The first aspect is *the lack of transparency in governance processes,* which means failure to provide stakeholders with proper access to relevant information. Access to information by favoured actors results in a black box decision related to other actors but is decided without consent.
The second aspect is *the unequal representation of stakeholders*: Favoring governmental actors to provide governance and excluding single private actors to have a say. The governments are in power and not part of the actors following this governance, only maintaining it.
The third aspect is *changing influence in creating international public policy*: by having only state actors involved in governance and not involving private parties.

Adaptive governance

Adaptive governance is an area of governance that overlaps with the previously described characteristics and issues of governance. The focus of adaptive governance is to specify emerging technologies and use new information to adapt the governance and reduce uncertainties within past governance (Brass & Sowell, 2020). The critical aspect of adaptive governance is to capture further details or challenges from the socio-technical system (IoT networks) and use this knowledge to redefine governance or even replace it. This requires an agreement between actors to iterate on governance instead of having a fixed arrangement. This includes a formal commitment to re-evaluate a governance decision, the use of new knowledge for an emerging risk, and capacities to use the further information (Brass & Sowell, 2020). This highlights IoT governance: having fixed governance, not adapted to IoT, and not evolving with innovative uses of IoT. This adaptiveness comes back in the aspect of accountability, transparency, and representativeness.

4.3. Current IoT governance

Looking at governance options to remediate vulnerabilities in IoT, there are public and private stakeholders involved (see table 4.2). This governance can range from international legislation to soft rules or norms. Specifically for remediation, there seems to be a focus on users themselves for remediation or internet service providers to take responsibility for remediation of vulnerabilities. The focus on manufacturers is more on technical solutions for remediation and not on governance instruments that force manufacturers to provide better remediation options. More on this in 4.3.2. Manufacturers: IoT issues, guidelines, and legislation.

Table 4.2 An overview of types of stakeholders and activities in governance (Jayawardane et al., 2015)

		Activity				
		Norm development (or contesting existing rules)	Norm dissemination and implementation	Agreeing on soft norms	Agreeing on binding international legal obligations (treaties)	Enforcing legally binding rules
Actors	States	X	X	X	X	X
	International/regional organisations (e.g. UN, ITU, EU)	X	X	X	X	
	Private sector organizations (such as businesses)	X	X	X		
	Civil society organisations (think tanks, advocacy groups)	X	X	X		
	Technical community	X	X	X		

4.3.1. Internet Service Providers and users

There are always the reoccurring device manufacturers, device users, and some authority actor in charge of 'governing' concerning stakeholders within IoT. However, within IoT literature, there is a focus on the facilitator of IoT usage: the internet service providers. These ISPs are described for facilitating network access for the internet of things and playing a vital role in reaching users through IP addresses. As passive network observers, they can collect IoT devices within their networks (Apthorpe et al., 2017). There is a privacy issue created by combining the novelty of IoT and the lack of current legislation and governance. The only governance recommendation from the literature concerning ISPs is that data collection needs to be specified when developing governance (Apthorpe et al., 2017).

This comes down to the issue of data ownership and the necessity of data. With different stakeholders requiring different data, data collection and sharing rapidly become a complex problem in terms of privacy regulations: making uncertain who owns the data collected by various stakeholders (Dutton, 2014). This is an issue of privacy versus control.

ISPs facilitate IoT infrastructure and can therefore contact their customers (whether that be consumers, businesses, etc.) since they provide the networks for usage. When it comes to solving vulnerabilities, even though ISPs have data on vulnerable devices, there are little to no incentives for ISPs to solve these vulnerabilities pre-emptively actively. (Cetin, Ganan, Altena, Kasama, et al., 2019) did a study into remediation efforts through ISPs to IoT device users. These remediation efforts all put the responsibility of solving IoT vulnerabilities in the hands of individual users by telling them: your device is vulnerable, please fix it before using our network again. Cetin, Ganan, Altena, Tajalizadehkhoob, et al. (2019) also found a lack of information to identify device owners, communication channels to these owners, and ways to provide actionable notifications. Together with a weak incentive from the ISP to act on IoT vulnerabilities, Cetin, Ganan, Altena, Kasama, et al. (2019) highlights the issue of having a multi-stakeholder situation, no clear

guidelines or options to act on through the data, and the question of which stakeholder can act with the data they can gather.

User awareness and efforts

The most effective solutions should keep user awareness and attitude towards IoT in mind (Zheng et al., 2018). Most users of IoT prefer the convenience of the IoT service and through this disregard privacy issues and potential third party usage of data (Zheng et al., 2018). This means that the idea of 'starting' IoT security issues at the user will not be practical since this highly depends on how the user perceives vulnerability: and most users seem to accept vulnerabilities by getting an IoT service in return. To show that these user attitudes might be wrong, the following characteristics were shown in smart home users (Zheng et al., 2018): the amount of data sharing users are willing to accept depends on the IoT service used, users expect well-known brands to be more secure than unknown IoT manufacturers, users believe only audio/video capturing devices gather data while every IoT device collects (meta)data that could show patterns.

Specified governance options to remediate software vulnerabilities can already be found in conventional IT systems. However, these options are mostly not applicable to IoT vulnerabilities because of most IoT devices' (lack of) technical capacities. For instance, sending out notifications to update a device is problematic since most IoT devices lack a decent interface or friendly software design to give actionable notifications. Imagine having to update a router without an interface or a smart light bulb: it was found most users lack the technical knowledge to do this (Perera et al., 2014). If, hypothetically speaking, the device user or owner can be found (through IP address, for instance), then ISPs are the only actor that can legally contact these users. Sending out an email notification can work, but it is shown to be not effective (Cetin, Ganan, Altena, Kasama, et al., 2019) since users can still choose to ignore this information. Having a device install software updates automatically seems like the right solution, also because it puts the responsibility of having a software safe device in the hands of the manufacturer instead of the users. However, most cheap IoT devices lack the technical capacities to install automatic updates, and this also requires maintenance from the manufacturer to keep the device updated.

Having an infected device quarantined in the network it is on, until the security issue is remediated is an effective method to solve software issues or device misconfigurations. ISPs mainly do this, and these devices are put in a 'walled garden' that they can only be released from once the vulnerability is remediated (Cetin, Ganan, Altena, Kasama, et al., 2019). Even though this seems like a suitable method, it does put the burden of a vulnerable device on users while it might not be a user's responsibility. Unsecure devices by design should not be a user's responsibility to fix.

This highlights responsibility and available options: what stakeholder has the information and capacity to act. To protect users of IoT, there is a *"misalignment between risk-based regulations for product safety and security; and growing information asymmetries between consumers, IoT manufacturers, and digital service providers."* (Brass & Sowell, 2020, p. 6)

4.3.2. Manufacturers: IoT issues, guidelines, and legislation

Conventional regulations for consumer goods take a regulatory risk approach, which consists of creating standards and product regulations based on a trade-off consisting of all potential risks mapped (Brass & Sowell, 2020). Regarding current legislation and governance, some initiatives include IoT guidelines targeted towards IoT stakeholders to ensure IoT security (Abdul-Ghani & Konstantas, 2019). However, when asking the IoT industry itself, they believe that current data legislation is enough for safe IoT usage, while most users and consumers prefer more specified security regulations (Weber, 2013). This indicates multistakeholderism with two different perspectives and the need for specific governance. Manufacturers are required to comply with set standards or regulations. However, these regulations can only be set when the risks and uncertainties are clear. Considering the diversity of IoT and innovations in IoT, creating specific regulations for manufacturers is a challenge (Brass & Sowell, 2020).

Within IoT, Wachter (2018) identifies the following main challenges in terms of regulation:

1. Invasive profiling by relating user information from IoT services together, leading to data profiles of users.
2. Sharing of data against the user's will, through other IoT services or with other involved actors. Giving the user no control over their data.
3. The development of data or data interference that gives more information about the user is against the user's will and was not agreed upon in user policies or access to the service.
4. No transparent data handling and not viewing your private data as a user means that you have no insight into the data. This leads to trust issues and can lead to data leaks of sensitive user information.

The European aspect: GDPR and ETSI

The most' famous' regulation that relates to IoT legislation is the General Data Protection Regulation (GDPR) set by the EU, set up to protect the personal data of individuals. It entails details about informed consent, privacy by design and default settings, impact assessment, transparency, and machine learning (Wachter, 2018) explicitly. This legislation gives more clarity on privacy protection. However, it is not targeted towards the data collection behaviour of consumer IoT (Zheng et al., 2018). Wachter (2018, p. 4) says that the GDPR is *"insufficient to ensure a fair balance is struck between user's interests in privacy and the interests of IoT developers and data controllers"* due to lack of specification into IoT. These guidelines lack compulsory implementation or accurate specification (Abdul-Ghani & Konstantas, 2019) and are shown to be mostly ineffective for IoT devices. Even before the GDPR, the European Commission set out 14 guidelines for the IoT developers (Weber, 2009). The list addresses technical solutions and governance. Relevant aspects for this research, meaning in terms of governance and legislation and not purely technical measures, are:

1. Governance: decentralised management and general principles for development,
2. Privacy and data protection principles,
4. Identification of emerging risks through a policy framework,
5. Standardisation and protection of critical information,
8. Setting up public-private partnerships is essential,
10. An increase in institutional awareness
14. Setting up a multi-stakeholder aspect and monitor IoT through these stakeholders.

This highlights the different institutional (and therefore governance) challenges. However, full (compulsory) implementation of these principles in real life has not occurred yet. The main question is whether there can be a 'concluding' governance option that solves IoT issues for good. The emergence of compulsory IoT standards has created a fragmented mix of IoT security standards, guidelines, and regulations. This highlights the coordination issue of IoT governance, with no specific rules to follow (Brass & Sowell, 2020).

A continuation of these guidelines is the ETSI 303645 (European Telecommunication Standards Institute) IoT security standard of 2020. Consisting of 13 requirements for manufacturers to implement (no default passwords, force security updates etc.), this standard can be used as a basis for certification or setting technology standards (ETSI, 2020). For instance, as input for the Radio Emission Directive (RED) that certifies every radio signal emitting device in Europe. However, the same issue still occurs: these guidelines are non-binding at the moment, aimed at manufacturers, and quite general in a security sense. There is currently no legislation that incorporates these, and also no possibilities to monitor for compliance.

To effectively tackle IoT vulnerabilities, continuous governance improvement should involve the full spectrum of involved stakeholders: starting at development and manufacturing and ending at the end-user (Abdul-Ghani & Konstantas, 2019). Through hardware improvements, software fixes and improved update mechanisms, the manufacturer is responsible for IoT security, but through safe usage and configuration, password updates, and manual software updates, the user is also responsible for device security (Abdul-Ghani & Konstantas, 2019).

Non-specific governance

The heterogeneity in IoT technology and the multi-stakeholder aspect creates the issue of 'non-specific governance'. According to Weber (2013), specific IoT governance is unnecessary since cyber or internet governance is already in place, and new IoT technologies should incorporate these regulations and comply with current governance. However, this will not change the current situation and issues highlighted.

Security and privacy have to be designed and put through on a policy level and through legal terms and conditions (Perera et al., 2014). Governments are the central actor to ensure security and privacy by developing data protection, privacy, and customer protection laws specified to IoT (Abdul-Ghani & Konstantas, 2019). For instance, certification programs that set IoT standards concerning privacy (anonymization, encryption, data sharing, etc.) for IoT manufacturers are evaluated through guidelines (Zheng et al., 2018). This would require manufacturers, governments, and device users to design this governance.
Through this the multi-stakeholder aspect of IoT will have to be more mobilised to apply these laws. The dilemma in this results in IoT services and devices being used and the need to check these devices, limiting usability (Abdul-Ghani & Konstantas, 2019). This is a social challenge within IoT since the devices and services have to remain accessible and usable while also keeping a check on the involved stakeholders. This can contradict each other and highlights the need for specific governance instruments. Preferably through automation, user awareness (Apthorpe et al., 2017), or little reliance on users, since the most sensor and device owners are believed not to be technically skilled (Perera et al., 2014). These different types of options need to be structured.

4.4. Structuring governance: framework typology

To structure governance options a typology of hierarchies, networks, and markets can be used (figure 4.2). Defined by Kuerbis & Badiei (2017), a framework with these three categories of governance is provided:
Markets: "Transactions among actors are driven by information and price mechanism, and enforced by law and contract." (Kuerbis & Badiei, 2017, p. 5). For IoT, the best example for this is the need to deliver an IoT device at a low cost that is safe enough to be sold to a consumer. If a device user is unaware of vulnerabilities a device might carry, he or she might be more willing to buy it.
Hierarchies: "Governing structures by which actor(s) transactions are compelled by an authority" (Kuerbis & Badiei, 2017, p. 5). An example for IoT can be an authority setting standards that manufacturers have to follow during production and enforced through sanctions.
Networks: "Semipermanent, voluntary negotiation system that allows interdependent actors to opt for collaboration or unilateral action in the absence of an overarching authority" (Mueller et al., 2013, p.89). Concerning IoT, an example would be internet service providers collaborating only to allow devices that live up to a standard onto their networks. Within networks, collaboration is the keyword.

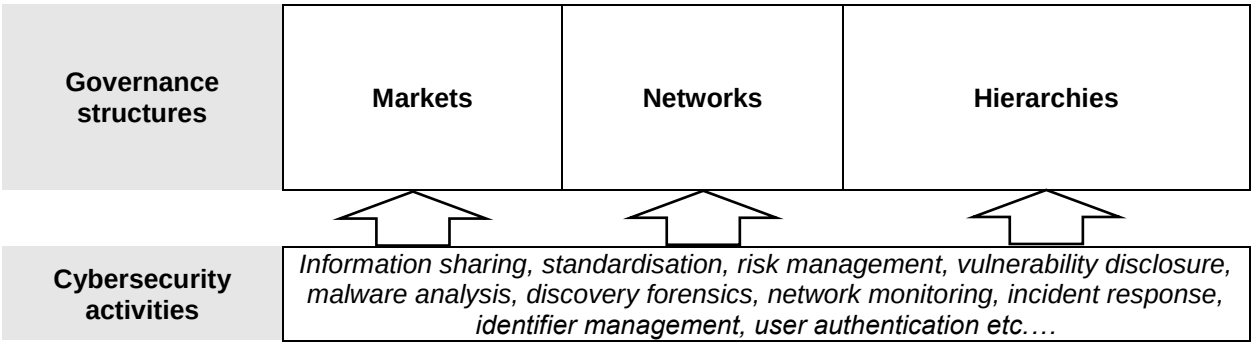

Figure 4.2 The framework defined by Kuerbis & Badiei (2017) to structure cyber governance.

This framework topology will determine different types of governance options in chapter 9 of this research.

4.5. Principles of IoT governance

To design governance that is effective for IoT, a set of principles will be defined. Based on the governance literature described a set of principles is taken that, when applied correctly, solves the issues described previously.

Trust and usability

The overarching principles that relate to every aspect of governance can be seen as trust and usability. This includes trust in the stakeholders to define governance, trust in IoT itself, but also trust in an overseeing actor that controls your data as an IoT user (Roman et al., 2011). For every principle deemed important for effective governance, there has to be a basis of trust between stakeholders and between users and the IoT service or device they are using. If governance mechanisms are designed to keep relevant governance principles in mind (transparency, accountability, representativeness, security and confidentiality), there is no trust between the user and the IoT service. This governance mechanism undermines the actual usability of the IoT service. The same holds for usability: if the most effective governance is designed in terms of principles and safety, but the IoT service becomes unusable, then the designed governance also becomes not implementable. Therefore trust and usability are defined as the most relevant principles to return in every other governance aspect.

Transparency

Transparency and access by the user, giving users transparency into the governance involved and the data gathered or required from them (Weber, 2009). It is defined as the broad concept of designing governance or governance options in an open manner and giving relevant involved stakeholders a look into what data (relevant to them) is used for what aspect (Jayawardane et al., 2015). This overlaps with lawfulness, which says to have legitimate grounds for the processing of personal data (Wachter, 2018). By making users aware of what data is processed and informing them about this process, lawfulness can also be tested.
The dilemma exists between informing users about the processing and acquisition of their data and keeping the service aspect and usability of IoT services (Wachter, 2018). This could also include trivial aspects like accepting data sharing every time you use a device: making it transparent but giving the IoT service less usability.

This principle is quite general, but considering the transparency in data collecting, it is more specified towards ethics and involves user consent and giving users the right to look at their data and delete it (Weber, 2013). To further define transparency Weber (2013) provides five parts that are characteristics of transparency in IoT governance:

1. An available stakeholder with the capacity to control or allocate the resources.
2. Reliable information that is publically available, with the ability to influence the governance design through preferences of other actors.
3. The definition of a receiving actor is the receiver of governance concerning information and transparency
4. Sufficient information concerning standards for information, right to access information, and to disclose information.
5. Keeping time and visibility of information in mind.

The concept of transparency also relates to limited data gathering and the purpose of data gathering. By making the data more transparent to the user, the purpose of this data will also have to be justified. Ensuring more limited data gathering and data minimization (Wachter, 2018).

Accountability

The existence of multiple stakeholders requires accountability within IoT governance (Jayawardane et al., 2015). Since IoT usage comprises data collection and sharing between stakeholders. There needs to be accountability regarding data usage and sharing: making different stakeholders responsible for collecting or sharing data. Therefore, it is accountable when this data leads to wrong conclusions or malicious actions. An overlap between transparency and accountability could lead to stakeholders being held accountable for collecting data they are not even supposed to be collecting. This full accountability of actors has to be improved through governance (Weber, 2013). To have leading governance in place that ensure accountability also provides some form of standard for how actors collect, handle, and share data (Weber, 2009), creating a precedent.
Related to accountability is the accuracy of the collected data, meaning it has to be accurate for the purpose it is collected for (Wachter, 2018). Since conclusions can be analysed from data, the stakeholder collecting this data should be held accountable for findings resulting from this data.

Representativeness

Governance structures serve as guiding mechanisms to govern public and private actors. In this way, governance also has to represent the stakeholders involved. By representing the stakeholders involved somehow, through governance design or active involvement, the effectiveness of governance measures will also improve (Jayawardane et al., 2015). Involving or representing the right stakeholders can also lead to opportunity structures, defined as *"the co-evolution of technology and social institutions, which sequentially or simultaneously generate opportunities for change that agents might take"* (Borrás & Edler, 2014, p. 26). This indicates that the involvement of the right actor leads to more effective governance. Therefore governance of IoT should be framed as not as a design decision by a public actor, but recognising the knowledge that comes from "*day-to-day operational experience among those who deploy, operate, and manage them on the ground."* (Brass & Sowell, 2020, p. 16). For instance, the inclusion of private actors or civil society when designing governance instruments, since governance of IoT is about the way IoT in society is used (Jayawardane et al., 2015).

Security and confidentiality

The most apparent but essential principle for effective IoT governance has to ensure security and confidentiality. Even if all rules, legislation, governance structure, and actors are involved, this could still infringe with security measures. For instance, full transparency of data would also involve security risks in terms of data sharing. Therefore security is an essential governance aspect that must be defined in some form of standards specified towards IoT (Jayawardane et al., 2015). To make this tangible: the forming of extensive personal profiles will always result from IoT usage; therefore, data anonymisation should be part of the equation (Weber, 2013). At the moment, IoT design is centred around the service, and the data collection is deliberately done unnoticeably by the user to increase the service aspect (Wachter, 2018). This also relates to transparency, but when IoT stakeholders handle confidential data, they need to have appropriate security mechanisms in place to ensure access control and prevent data leaks or breaches (Wachter, 2018).

4.6. Conclusion

From the overview of IoT governance and the current guidelines and issues involved, a selection of principles was made that will ensure an effective design of governance options. By doing this literature review and defining these principles, the question is answered: What principles from current governance applicable to IoT devices can be learned from literature? The recurring conclusion seems to be taking away responsibilities from IoT device users and making sure that through multi-stakeholder decision-making, specific stakeholders can be appointed to have more insights into IoT and involved problems to create and enforce better governance decisions and legislation. This means network governance (Kuerbis & Badiei, 2017) seems most applicable.

This results in governance aspects categorised by the governance of change pillars defined by Borrás & Edler (2014), with related governance principles used in chapter 8 as guiding principles to see what governance options are valid. An overview of findings is found in table 4.3.

Table 4.3 An overview of concepts from literature.

Aspects of governance of change (Borrás & Edler, 2014)			
Capable actors: *Who drives change?*	**Instrumentation:** *Governance structures & Principles*		**Why is it accepted:** *Legitimacy*
- States - International/regional organizations - Private sector organisations - Civil society organisations -Technical community ➔ *Multistakeholderism*	Governance structure (Kuerbis & Badiei, 2017): - Markets - Hierarchies - Networks	Trust and usability	General principles that are required for governance to be implementable.
		Accountability	Ensuring the stakeholder collecting or handling the data is accountable for any actions resulting from this. It also provides a justification for collecting data.
		Representativeness	Ensuring the right actors are involved in the governance design or the right actors represented in some way for an effective governance outcome. Results from the multi-stakeholder aspect.
		Security and confidentiality	The main principle behind the development of IoT governance that needs to be ensured.
		Transparency	Ensuring transparency in what data is handled by who and why. Also making sure access is controlled.

The concepts of this literature review provide background information for the governance landscape of IoT. The next steps will be using the presented concepts in table 4.3 to categorise the governance defined in chapter 7 and 8 and use the information to create a conceptual framework in chapter 9.

5 Network scan data

The use of empirical data to answer the main research question provides a real-life context for IoT devices. For this empirical data, a network scan dataset is used to determine what information is available to identify IoT devices, vulnerabilities, and stakeholders. Using this dataset, the following sub research question will be answered: What information in terms of devices and stakeholders can be found in the scan data of The Hague? To answer this question, the origin of this dataset and information found from the dataset will be addressed, which will be used to assess what can be concluded from the empirical data. Characteristics for good security metrics (Jaquith, 2007) will be used to see why information found is or is not applicable.

The main goal of this chapter is to uncover what (and if) the available data is capable of identifying security issues, stakeholders, and device information. Through answering this question, the context for defining governance options will be made. The goal is not to identify specific devices and stakeholders by name, since in terms of content, the data differs per device (Fagan et al., 2020). The goal is to see what is possible in terms of identification. Specifically, looking into the data per device would be impossible and possibly illegal due to reading personal information.

5.1. Origins of the network scan dataset: Cybersprint

The dataset used for this consists of 1649 IP addresses, collected by Cybersprint through scanning public networks. Cybersprint is a Dutch cybersecurity company specializing in attack surface monitoring. Scanning, identifying and monitoring online systems is a central part of their service offerings. The identification and inclusion of IoT is a novel part of their business. Consequently, they are more actively trying to identify IoT devices from the scan data they collect. However, this way of scanning networks and collecting data for the dataset used causes a data bias which will further be addressed.

5.1.1. Data collecting

To collect the data on IoT devices, the following steps are performed:

1. **Portscan the whole IPv4 space of the internet and part of the IPv6 space**
   Cybersprint's scanning infrastructure scans all IPv4 addresses, but since scanning all IPv6 addresses is not possible, pre-identified IPv6 addresses are used. This refers to IPv6 addresses that already left traces online (e.g., already published or linked to a server, for instance). This list of IPv6 addresses is then also portscanned. To add to these scans, they use information from scan sources like Shodan and Censys.
2. **Determining active services**
   Services found on the IP addresses from the scanned networks. Inactive services or inactive IP addresses are not used for the dataset.
3. **Limit the scope to the city of The Hague**
   For this project, the identified IP addresses are matched against GeoIP data and geographically filtered to include only results from the city of The Hague.
4. **Filter the remaining results based on rules and heuristics**
   Cybersprint has to write these selection rules for specific devices. Based on a combination of heuristics, devices are identified. Some types of devices offer more specific information, and not all devices show this information by themselves. For instance, if the web page's source code has a fixed and specific structure, there is a login function, a video stream, the name of a known webcam supplier, software version, etc. This information is combined to conclude if the device is a webcam, for instance. If it can be concluded what device it is, then the device is added to the database.
5. **Fingerprint the identified devices**
   Determine the type of device and the software/firmware version of these devices, and then add the IP address to the database.

6. **Go through the added IP addresses and add vulnerability or risks**
   Based on the fingerprint information, the Common Vulnerabilities and Exposures (CVE) database is used to assess the security risks present on the identified webpage or IoT device belonging to the IP address.

The dataset then consists of IP addresses with, if available, also a list of active services, certificate information, domain information, and network information belonging to this IP address. Devices are only identified at a small number of IP addresses in the database and contain device brand or software version. In the database most IP addresses belong to a webpage and include a screenshot of this webpage or interface.

5.1.2. Data gathering methods

The sources these IP addresses are collected from are the entire IPv4 address space (4.2 billion) and a part of the IPv6 IP addresses that are pre-identified. The scan data and results belonging to each IP address are collected and compiled from public and non-public data sources. These data sources are correlated to get a complete picture of the IP address. For this research, the focus is on publically visible IoT devices visible in the network scan data. This already indicates the question of whether the information visible belonging to these IP addresses and the devices found at these IP addresses should be publically visible.

When it comes to data sources the following are used:

Cyber map

The primary source of data on the IP addresses is Cybersprint's own network and port scanning infrastructure called Cyber map. This is based on an open-source network scanning framework. Information resulting from Cyber map is supplemented with Shodan information.

Shodan

Public search engine that collects data on connected devices accessible through the internet (figure 5.1). This means any connected device that is publically visbile can end up in the Shodan data. The most important security issue within this data is the availability of a device or IP address within this public search engine. Since Shodan is located in another country (other than the Netherlands), they have to comply with different (less strict) legislation to gather IP data. Using Shodan as a loophole means you have to collect less data by yourself, decreasing the chance of violating legislation.

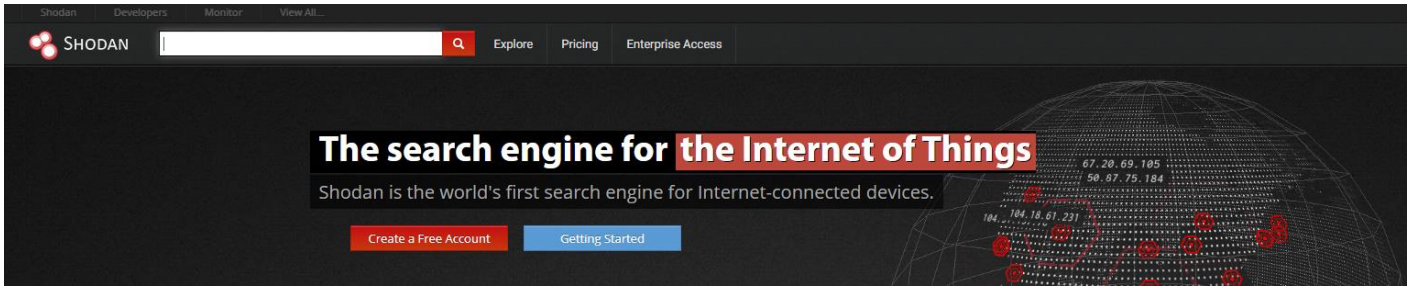

Figure 5.1 An example of Shodan, used to find IoT detectable on the internet.

5.1.3. Data availability

The collected IP addresses are scanned and the information is aggregated with IP data from GeoIP and WhoIS data (which will be discussed in chapter 5.2). The dataset consists of 1649 IP addresses at the moment of inspection, and IP addresses will only be added when a new scan on IP addresses is performed. This is not done regularly due to the high demand for Cybersprint's systems. If the services on an IP address become undetected or inactive, or if a device changes its IP, then the IP address will be archived and will be taken out of the dataset. So IP addresses and devices belonging to them will only be removed or archived from the data once they are undetectable or not able to be fingerprinted. This could also happen when an owner unplugs an IoT device or plugs in an unknown (not IoT) device. No IoT device will be detected on that IP address, and therefore the IP address will be taken off the IoT devices list.

Due to the prototype nature of the dataset, meaning identifying IoT devices from website IP addresses, there is no historical data available to compare the same identified IoT devices and security issues with historical data. This is caused by the selection and completeness bias that would require all scan information to be saved for every IP address at different points in time and processed retroactively, which is not done at the moment. This data bias will now be addressed.

The selection and lack of completeness bias

The empirical scan data is gathered from networks. Within the data, there is a data bias consisting of two aspects: The data does not contain all IP addresses of devices in the area of The Hague since only specific devices are taken into the data and identified based on the fingerprint rules. Cybersprint as data collector decides what devices they want to identify from the collected IP addresses and then writes rules to identify them; therefore, a deliberate choice must be made to include specific devices (and therefore IP addresses). The rationale for current devices in the dataset comes from a pragmatic point of view. From all data collected, they sift through the IP addresses and identifiable information belonging to this IP address. If they recognize features of these IP address they write code to detect these similar devices from these IP address, throughout the whole scan data. These identified devices ended up being primarily consumer devices being fingerprinted.

This means the data only contains devices with features they know beforehand, since for a device to be identified from the networks scan data specific selection rules have to be written. This means there could be a lack of different specific smart devices within the data since new rules or heuristics have to be written for such particular devices. This indicates a data selection bias since the dataset does not include all publically visible IoT devices. So it hinders consistent data measurements (Jaquith, 2007) that are essential for good metrics.

The second aspect of the data bias comes from the empirical point of view but relates to the selection bias. When looking at a specific geographical area, the scenario could occur that a single product (e.g. a router) is recommended to many consumers through subscription of the same consumer internet service provider. This relates to the rules needed to identify a device: once this device is fingerprinted in the dataset, there will be an overrepresentation of this device within the dataset since there is specifically looked for this device. This could give the impression that all people are using the same router while the router is only overly present in the data because it has been identified and fingerprinted. This is contextual specificity (Jaquith, 2007) that makes it difficult to reproduce the data gathering, and gives the data a bias.

5.2. Description of the network scan dataset

The dataset consists of 1649 IP addresses. All 1649 IP addresses result from websites or web interfaces publicly visible. This includes online login pages, and there are IoT devices linked to these web interfaces. From these 1649 IP addresses, information on IoT devices will be identified.

Why IP addresses?

Once an IoT device is connected to a network, it receives an IP address from the provider of that network (usually an ISP). Most IoT devices also have some (web) interface to control or set up the device, which has the same IP address as the IoT device. These web interfaces are run from the IoT device itself and are mostly not accessible from outside the network. This means that you can access the IoT device once you are connected to the same Wi-Fi by going to the IP address or domain name belonging to the device in your browser. Being able to access the domain or web interface belonging to the IoT device results in different security issues than finding IoT devices without web interface. An example of various aspects belonging to an IoT device is shown in figure 5.2.

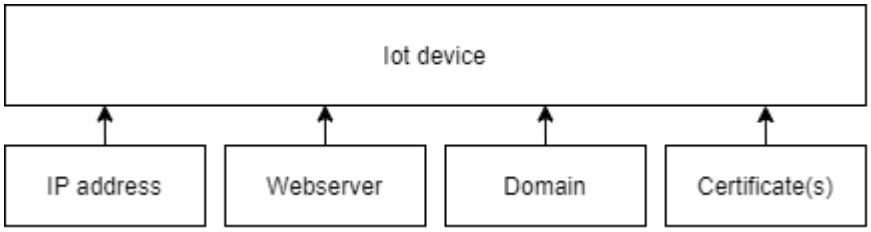

Figure 5.2. An example of different aspects an IoT device can be categorized on.

For example, by looking at domain-related security issues (e.g. the website or web interface belonging to the IP address), there will be different security issues than an IoT device by itself. The assessment of the security risks present in the IoT devices and its different aspects is done using the CVE database, which will be discussed in the following section.

5.2.1. Common Vulnerabilities and Exposures (CVE) database

The Common Vulnerabilities and Exposures (CVE) database is used to identify vulnerabilities in the dataset of IP addresses. The IP addresses is only an identifier, and can not be safe or unsafe. The web interfaces and devices belonging to these IP addresses can possess security risks. For each IP address the information of the corresponding device or web interface gets a rating based on the severity of the security risks found in the CVE database and other known risks. Vulnerabilities in the CVE dataset are provided with a CVSS (Common Vulnerability Scoring System) score, ranging from 0 to 10. This score is taken into account in the Cybersprint rating, which ranges from A: meaning no known problem at the moment, to F: critical problem(s) identified. So a CVSS score of 10 results in an F, for instance. This rating in letters is developed and used by Cybersprint.

An overview of the different security risks within the dataset can be found in figure 5.3. These risks are not definitive as in to say: a security rating of A means a web interface or device is safe. Currently, it only means there are no known risks based on the available data used to determine this risk. Looking at the most significant risks, sixty IP addresses are identified to possess aspects with the highest risk (F). These all result from vulnerable software on the server the corresponding website is run from. This automatically classifies them with the highest CVE score since malicious actors could use software vulnerabilities to access the system, compromising the security of the entire network the IP address of the website is part of. Apart from those vulnerabilities, another aspect is whether this information belonging to the website or device (and therefore IP address) should be publicly accessible (the reason it ended up in this data). This means it could also be viewable by a malicious attacker as well, increasing the risk to have security vulnerabilities exploited.

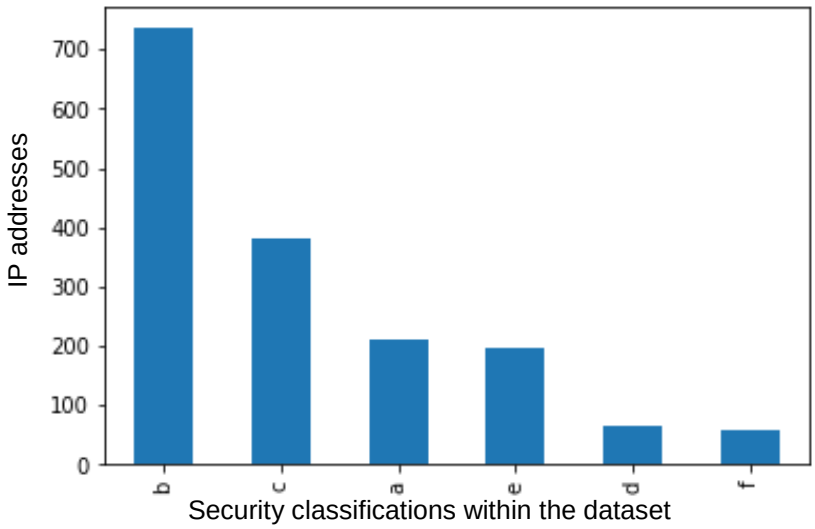

Figure 5.3 The number of IP addresses with different security classifications based on web interfaces or devices belonging to the IP addresses, within the dataset.

However, within the 1649 IP addresses, there are IoT devices that can be identified. This is where two different perspectives can be used: looking at the IoT devices belonging to an IP address, the IoT device can be classified as A with no risks found on this device. At the same time, the web interface of the same IP address can be looked and be classified as security risk E, with vulnerabilities resulting from the web interface and the fact that an IoT device is detected. This would give the impression that IoT devices are safe, but the related web interface or domain belonging to the same IP address as the IoT device possesses security vulnerabilities. However, the ability to detect the IP address of an IoT device, identify the technology and software of this device, and get to the web interface and attempt to log in is a vulnerability. This makes the presence of an IoT device in the dataset and the identifiable fingerprint information already a vulnerability by itself. The found vulnerabilities on the domains (meaning: as an IoT device there are no vulnerabilities, as a website or domain it has vulnerabilities) create the ability to use domain-related vulnerabilities as a way to gain access to the network and the IoT device (figure 5.4). Therefore, saying the 'IoT device has no risks' is preliminary since it is linked to a website or domain with vulnerabilities.

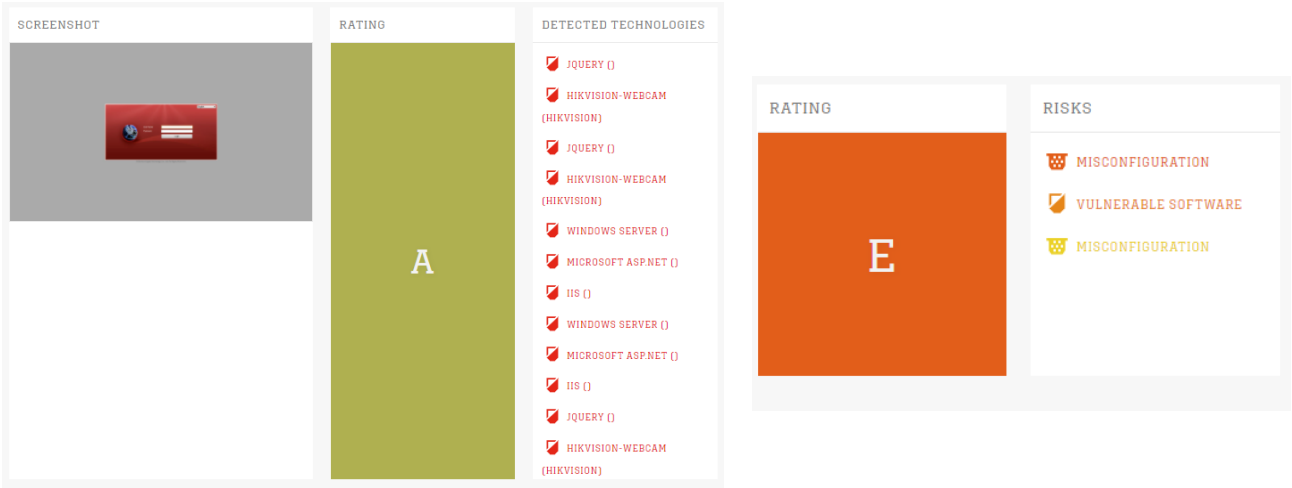

Figure 5.4 An example of the same IP address, with the same webcam, being classified with a different security rating depending on a domain or IoT perspective.

5.2.2. Finding IoT devices within the IP addresses

Within the dataset of 1649 IP addresses that are thought to belong to IoT devices, only 191 IP addresses are identifiable as IoT devices. The remaining IP addresses either belong to domains that initially could have belonged to IoT devices but now are reserved or not being used (anymore), websites not belonging to an IoT device (e.g. a webshop), or an IP address belonging to a different service like a general web server or email server. Of the remaining 191 IP addresses belonging to devices, there are 62 devices fully fingerprinted, meaning that they are identified with a level of confidence and assessed in terms of security risk. The remaining 129 IP addresses belonging to devices have identifiable information (web interfaces can be accessed for instance) but are not yet confirmed and assessed as IoT device with certainty. The certainty of which a device can be identified from these 62 IoT devices is >90%. This means there is almost complete certainty about the kind of device, based on the information and web interface belonging to the IP address. There is no middle ground or doubt: once a device has been classified as 'webcam' or 'lighting', it is >90% certain. However, there is still some uncertainty concerning software, web server, or operating systems of such devices. This is highlighted in the data with a percentage to indicate parts of the device information that is still uncertain (figure 5.5).

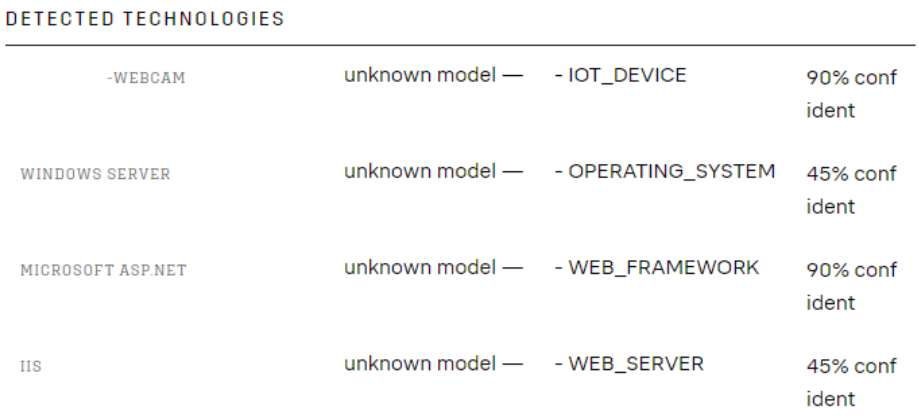

Figure 5.5. A detected webcam from the scan data, with confidence percentages.

As explained before, there is a difference between looking at websites belonging to the IP addresses and looking at devices belonging to the IP addresses. This shows when comparing the 62 IP addresses of the fully identified and classified IoT devices against the same IP addresses classified as website (see table 5.1).

Table 5.1 Looking at the same IP addresses through different perspective indicate different risks.

The difference in perspective: IP address security risk vs IoT security risk		
62 IP addresses (from the total of 1649)	Viewed as IoT device: 62	*Security risks identified:* A *(no known risk)* → 62 (100%)
	Viewed as a website: 62	*Security risks identified:* A *(no known risk)* → 10 (16,1%), B (small risk) → 9 (14,2%), C (significant risk) → 1 (1,6%) E (second highest risk) → 42 (67,7%)

The biggest takeaway is that a device by itself might have no known risk, but is has an accompanying login page, related web certificates, web server, or domain belonging to this login page, which then creates security risks for the IoT device. The most significant vulnerability is being able to identify an IoT device and device information from the IP address.

5.3. Data analysis: what does it tell?

There is information belonging to the IP address concerning location, type of device using this IP address, and common vulnerabilities belonging to the web interface or device. From this information, conclusions will be made on what IoT device information can be identified, what information will lead to identifying specific stakeholders, and what information will lead to a dead end. Characteristics of good security metrics by Jaquith (2007) will be used to conclude why the data is (in)sufficient.

5.3.1. Locating an IP address

GeoIP

By using the GeoIP database, estimates of IP address locations can be found. Using specific IP locations can, in theory, be used to create potential clusters of devices in a particular area. The IP addresses in this dataset are all centred on the area of The Hague. There is, however, a catch since this is not 100% accurate. Technically it is difficult since there is no way to map physical location of a system to the IP address. Also, due to regulations (like the GDPR, see 5.3.2.: WhoIS: identifying users from IP address) it is not even allowed to pinpoint a location based on an IP address, even if it was technically possible. The closest you can approximate it is the network of the ISP the IP address is originating from, which only gives you a general area. Another reason that could explain outliers in terms of IP locations is the market for IPv4 and IPv6 addresses, mainly since new IPv4 addresses have run out. This means that money is made selling (used) IP addresses, therefore potentially also changing the location of these IP addresses. This could explain why a part of the websites belonging to these IP addresses were initially active and categorised to belong to an IoT device when added to the dataset, but when looked at now are now used by other services (e.g. webshops). Some locations of IP addresses can be considered an outlier (see 5.3.1.: Outliers), or inactive. All together these aspects create uncertainties in terms of locating IP addresses.

Can you locate an IoT device?

The implication of the lack of specificity and the uncertain location of some IP addresses creates a dead-end in terms of locating IoT devices. There is no specific location or area to be highlighted where there are more or less vulnerable devices. In combination with the data bias (as previously addressed), location information does not provide enough information. As shown in figure 5.6, most of the data comes from the Netherlands, specifically centred on the area of The Hague. This is the scope of the data, even though some IP addresses seem to originate from different locations. These outliers and exceptions will be addressed.

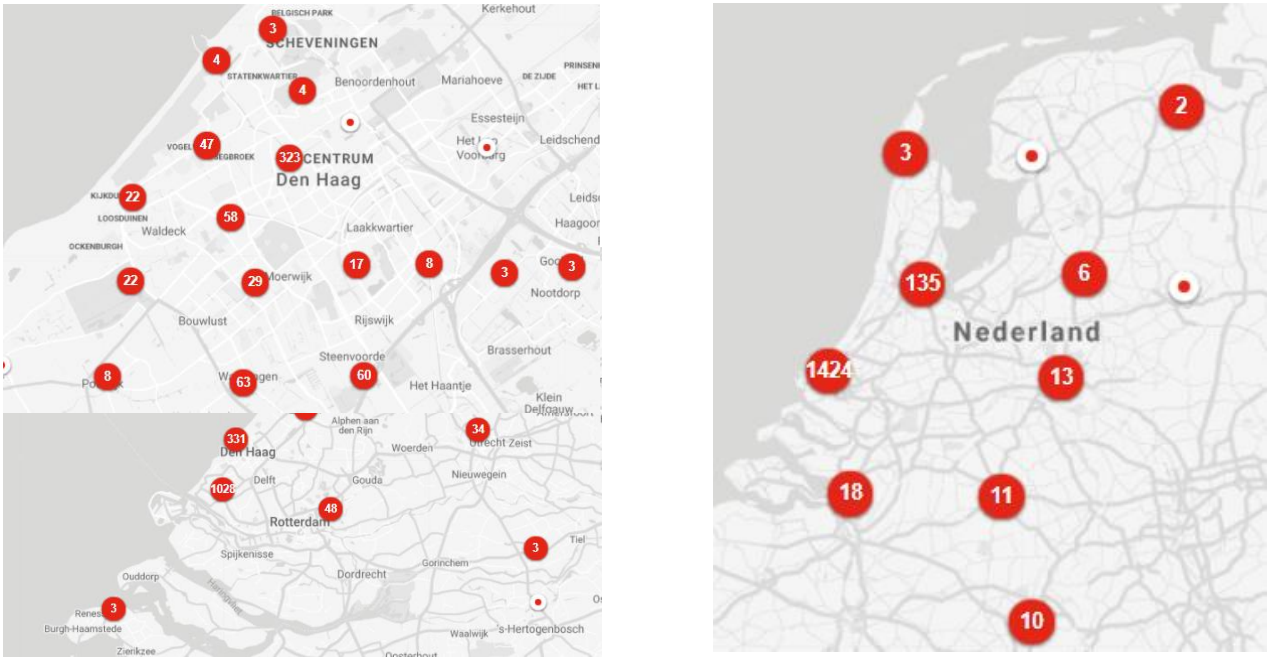

Figure 5.6. Screenshots of the general locations of IP addresses.

Regarding security metrics, this shows inconsistent data measurements (Jaquith, 2007): if you were to reproduce the dataset and look for IP locations, you might find different locations again. It also puts the discussion on the methodology (finding locations through GeoIP) instead of on the findings (Jaquith, 2007).

Outliers

There are IP addresses that seem to originate from The Hague, but when looking at the GeoIP database it indicates a different location (table 5.2). Within the data, the GeoIP dataset is used to go from all scanned IP addresses to only local IP addresses within the area of The Hague. It could be possible that the GeoIP database is not updated and therefore indicates the wrong area or country, an IP address added to the data is sold between correlating the scan data with the GeoIP data, or an IP address is just being used elsewhere after having been added to the dataset. This means that the data, even though scoped towards The Hague, then shows an IP address from a different area (or internationally).
There are, for instance, seven IP addresses found in the United States that seem European or Dutch but, through GeoIP, show up in the United States (e.g. *https://arbeidsmarktkansen.nl*, *http://www.crocs.eu*). These international IP addresses can be considered outliers in terms of location, but are not identified as 'belonging to an IoT device', and therefore will not be relevant to identify IoT device information for the scope of this research.

Table 5.2. Locations of IP adressess

GeoIP location	Instances
Netherlands	1624
Germany	10
United States	7
No information	4
United Kingdom	3
Russia	1

5.3.2. WhoIS: identifying users from IP address

Collecting data from Dutch public networks has boundaries due to privacy legislation and the General Data Protection Regulation (GDPR). The GDPR does not distinguish between publicly available data and private data: the GDPR applies to any data with potential personal information. The WhoIS database used does not contain personal information. There are IP and domain related WhoIS records. For IP addresses only information on the ISPs can be found. For domains the names of natural persons can be found in the WhoIS records. When relating the network scan data to the WhoIS data, domain-related WhoIS information is given related to the provider and ASN or IP related information, containing the name and contact information of the ISP. However, hypothetically being able to identify a user of a device from its IP address is not possible without consulting the ISP, since otherwise it violates the GDPR.

The only available WhoIS information to be found on the IP addresses are technical or administrative details. In this information, the internet service provider responsible for giving out the IP address or domain is shown. Since WhoIS information in this sense is used to address security issues about the domain or IP to the provider, the abuse team of most providers is listed as the WhoIS name or administrator. Any specific personal information is not exposed through scanning these networks and can not be found through WhoIS information.

5.3.3. Device types and security risks

Within the dataset of 1649 IP addresses, there are 191 IoT devices identifiable from these IP addresses (including 62 fully identified and fingerprinted). The following types of devices can be identified from the 191 IoT devices (table 5.3).

Table 5.3. The identified device types and numbers in the dataset.

Technology		**Total number in dataset**
Webcams		38
Routers		99
Hard drives		47
Smart home IoT devices	Energy management	4
	Smart lighting	3
Total:		191

Within these devices, there are identifiable vulnerabilities. These vulnerabilities are examples of risks per type of device that are viewable or identifiable through public access. These vulnerabilities are found in table 5.4.

Table 5.4 The vulnerabilities found on the devices identified in the dataset.

Technology	**Vulnerabilities found**
Webcams	- Operational Technology (OT) device detected - X-Frame-Options header missing from web interface - Vulnerable software found running the web interface - SSL Certificate not valid on web interface
Routers	- Operational Technology (OT) device detected - HSTS header missing from web interface - SSL Certificate not valid on web interface - X-Frame-Options header missing from web interface - Vulnerable software found running the web interface
Hard drives	- Operational Technology (OT) device detected - Vulnerable software found running the web interface
Smart home IoT	- Operational Technology (OT) device detected - SSL Certificate not valid on web interface - HSTS header missing from web interface

The main recurring vulnerability is the ability to detect an Operational Technology (OT) device. That means it is possible to identify a device by scanning that IP address. The main vulnerability with any of these devices is that these devices can be detected through a network scan, creating a possible way into the network. This vulnerability is found through the web interface coming from the device and being detectable from outside the network(Lampe, 2014). An example security threat is Mirai malware that targets IoT devices for the use of a botnet attack. Through IPv4 network scanning the malware attempts to beak in with common network credentials (Guo & Heidemann, 2018). So even though a device itself can be safe, the ability to find the device is a vulnerability.

The other common vulnerabilities relate to the web interface that is run from the IoT device. Following the principle of least privilege: services and ports should only use what they need to use and not be open or have more privileges necessary to keep functionality and security in mind (DCMS, 2018). This web interface does not need to be publicly accessible, and that knowledge, together with these vulnerabilities, creates another way into the network for an attacker. The vulnerability concerning the *X-Frame-Options header* ensures the web interface or service is not put into another 'frame' and prevent clickjacking attacks from happening. The *Vulnerable software found* means that from the Common Vulnerabilities and Exposures (CVE) database, it is known that the software used to run the web interface from the device is vulnerable. This is common to be exploited by an attacker. The same goes for vulnerabilities related to *SSL Certificate (*Secure Sockets Layer), which ensures encrypted communication between web browsers and the server running the web interface. SSL is used as a global standard and given out by a third party Certificate Authority (CA) (SSL Support Team, 2019). Related to this is *HSTS,* HTTP Strict-Transport-Security, which uses SSL and ensures a webpage is only accessed through HTTPS and not HTTP. Prescribing the safest way, and therefore making it more vulnerable when this HSTS prescription is lacking.

An overview of the types of threats, general solutions, and responsible parties can be found in table 5.5.

Table 5.5 An overview of vulnerabilities, threats they cause, possible measures, and actors involved.

Vulnerability as named	**Type of vulnerability**	**Type of threat possible** *(Chapter 3)*	**Threat violates security principle** (*Chapter 3)*	**Solution and security principle** (Chapter 3)	**Actor**
Operational Technology (OT) device detected	Misconfiguration (device-related)	**Management/information security:** - Public access to vulnerable information - Break-in attempts through web interface	Privacy, Policies, Confidentiality, Integrity,	Restrict public network access (Usability)	Device user, ISP, or manufacturer
Vulnerable software found	Vulnerable software (webserver)	**Management security:** - Unauthorized access to the network (Data leakage, impersonation) - Public access to vulnerable information (Data leakage) - Man in the middle attack (Data transit) - Denial of service attacks through data injection (*NVD - CVE-2010-5298*, n.d.)	Privacy, Confidentiality, Integrity, Availability,	Update software (Usability and policies)	Manufacturer
X-Frame-Options header missing	Misconfiguration (domain related)	**Information security:** Clickjacking attacks (Data leakage, impersonation)	Privacy Confidentiality Integrity Availability	Turn on X-frame options on web server (Usability and policies)	Manufacturer
SSL Certificate not valid	Misconfiguration (domain related)	**Information security:** Phishing, data breaches, vulnerable data stolen (Data leakage)	Privacy, Confidentiality Integrity	Acquire an SSL certificate for the web interface (Usability and policies)	Manufacturer
HSTS header missing	Misconfiguration (domain related)	**Management security:** Man in the middle attack (Data transit)	Privacy Confidentiality Integrity Availability	Turn on HSTS header for the web interface (Usability and policies)	Manufacturer

As shown in table 5.5, do all threats violate at least one or more principles from the CIA triad (chapter 3) or other principles. However, these threats are initially aimed at the device user itself, not the ISP or entire network the device is on. Therefore these vulnerabilities initially only involve the user, after which devices can get infected and affect the network or ISP. The size of this problem will now be addressed.

5.3.4. The networks of the IP addresses and devices

When looking at the WhoIS admin details for the IP addresses of the whole dataset different types of network providers can be identified (see table 5.6). Since the 1649 IP addresses also contain general websites (like web shops for instance) there are also webhosting companies found (20%).

Table 5.6. The different types of network providers from the dataset.

Provided by	**Number of IP addresses**	**Percentage from total (1649)**
Internet Service Providers	721	44%
Businesses with own network	154	9%
Webhosting providers	325	20%
IT companies hosting web interface	168	10%
Not-active, broken, or provider unclear	281	17%
	1649	100%

Looking at the identified IoT devices from the dataset (191) it becomes clear that 180 (94%) of the devices are found in networks of Internet Service Providers (ISPs) (see table 5.7). The IP addresses are mostly supplied by consumer oriented ISPs (151; 79%) which is in line with the identification of the devices, since these are mostly consumer electronics. There is a small part coming from business oriented ISPs (29; 15%). A small number of devices also originate from company networks (6; 3%).

Table 5.7. The different types of network providers from the identified devices.

Network provided by	**Number of IP addresses**	**Percentage from total (191)**
Businesses with own network	6	3%
Undetermined or unclear	5	3%
Consumer oriented ISPs	151	79%
Businesses oriented ISPs	29	15%
	191	100%

5.3.5. The size of the problem

Looking at the amount of data available, it is difficult to define the magnitude of the problem. The available dataset only shows a fraction of the total number of IP addresses, and a smaller number of devices identifiable from these IP addresses. The number of identifiable IoT devices (191 of 1649 IP addresses) seems like a small amount. The uncertainties lie in the fact that not being able to detect or find a device does not mean this device is safe, which could indicate there are many more devices vulnerable found in this dataset. The data also has a heavy data bias when selecting the IP addresses for the dataset. There are vulnerabilities found for the 191 IoT devices resulting from the dataset that do indicate common security issues with IoT devices. To put this into context: a webcam identified in this data, for instance. The only boundary to prevent malicious actors from being able to control this webcam is a username and password. This can be acquired through other methods (social engineering, data leaks, phishing etc.), exploiting the other web interface vulnerabilities found, or through default login credentials (Lampe, 2014). Most users are held responsible for updating passwords and ensuring a safe password. However, this reliability on device management is mostly false hope. Most IoT users do not update their passwords regularly and even use default factory passwords (Quach, 2018). That means attempting credentials like: "0000", "1234", or "admin" are the easiest way for an attacker to find a way into such a webcam.

The publicly available IoT login screens (see figure 5.7) combined with a lack of updated passwords highlights IoT vulnerabilities. It is like having a default key in your hand that works on many doors and is now also being shown doors that the key could potentially work on: this increases the risk of an actual break-in. Combine this with the knowledge that the devices found also includes webcam brands that sell baby monitors and indoor cameras, indicating the risk for users.
Through this user risk, the networks are also at risk, compromising devices and through infected devices exploit a network. At this point, the risk transfers from device user to ISP as well.

Figure 5.7. A login screen found in the dataset.

5.4. Conclusion

The purpose of this chapter was to explore a dataset of network scan data to answer the question: What information in terms of devices and stakeholders can be found in the scan data of The Hague? The main goal was to uncover what information network scan data can provide about IoT devices and stakeholders. To diagnose or understand an area of application (Jaquith, 2007) based on the metrics in the dataset, which showed not to suffice. To conclude, through scanning IP addresses from publically visible networks, fingerprinting IoT devices from these IP addresses, and using different databases to add information about these devices, the following conclusions can be made to find identifiable information:

Location: the information found is a dead end. The locations are inconsistently measured (Jaquith, 2007) since IP address locations can change. There is no specificity possible to pinpoint exact locations. Identification of specific households that have multiple vulnerable devices is also not possible.

The use of WhoIS information: identifying device owners is not possible. The GDPR restricts access to personal information. Therefore, the only stakeholder identifiable from this database seems to be the internet service provider that gives out the IP address. In terms of identifying users, this is an unspecific measure (Jaquith, 2007) and therefore no use.

Device information: the *types of devices can be identified and the service providers belonging* to these devices. These devices carry common vulnerabilities. This can, however, be influenced by the data bias that causes the overrepresentation of single types of devices, which is again caused by the inconsistent data measurements (Jaquith, 2007), resulting from the fingerprinting of specific devices.

The security risks these devices carry: Risks can be found on the web interface belonging to the IoT device, and the detection of the IoT device itself is a risk. The CVE risks shown per device are uncertain, which means no definitive conclusion can be made if the found vulnerabilities are correct. You could classify this as a qualitative result (the confidence percentage) (Jaquith, 2007), but this metric is not optimal considering its uncertainty.
In terms of vulnerabilities themselves: The presence and ability to identify IoT devices in public networks have no purpose other than needing internet access to function. Public accessibility is not required and creates an entry point for security threat exploitation.

The networks of the IP addresses and devices: From the dataset it is possible to identify the actor responsible for providing the network the IoT device connects to, through the WhoIS admin information belonging to the IP address. For the identified devices these are 94% originating from ISP networks (business or consumer oriented ISPs). Further details on users can not be identified unless contacting such ISP. Only 3% is found in business networks, which is expected since most devices identified are consumer devices.

The magnitude of the problem: The dataset indicates there are vulnerabilities in IoT devices. The dataset also shows similar devices with similar security risks. However, no conclusions can be made on the magnitude since the dataset only contains devices specifically fingerprinted, resulting in inconsistently measured data (Jaquith, 2007). This means there are potentially many devices yet to be fingerprinted and included and devices that can not be found but are still at risk. Therefore no conclusions can be made about the magnitude of the identified problem, which makes the dataset lack contextual specificity (Jaquith, 2007). This also does not facilitate a discussion before and after the intervention, defining bad metrics to provide a number or percentages (Jaquith, 2007). The vulnerabilities found are all security risks for the device users. Only after these vulnerabilities are exploited by malicious actors or when the device is compromised do these risks also transfer to an ISP.

The main issue why the dataset does not provide adequate metrics is because the data's focus is on the methodology that derives the data (Jaquith, 2007), which takes the discussion away from discussing the results. Gaining more quantitative insights in terms of concluding number from the same dataset would give the ability to showcase the identified vulnerabilities involving IoT devices better.

Now that it is clear what information the dataset can give the next step is to identify what stakeholders come from the data or are involved and who should take the lead in solving these issues. This will be addressed in the next chapter.

6 Stakeholder identification

The expectation that network scan data would give the ability to identify devices and device users proved to be wrong in the previous chapter. Identifying involved stakeholders determines the type of governance action that can be taken and gives insight into what stakeholders should be in charge. Therefore, based on the data and the conclusions found in chapter 5, different stakeholders will be selected. Added to this will be stakeholders from literature to answer the sub-question: Who are the relevant stakeholders resulting from the IoT network scan data of The Hague and literature?

6.1. Stakeholders from the network scan data

There seem to be dead 'ends' in terms of stakeholder identification from the data: single users can not systematically be found through the dataset. The only identifiable set of stakeholders result from the device and the network this device is on. These stakeholders are:
- Device manufacturers
- Internet service providers (ISPs)

6.1.1. Device manufacturers

An identifiable stakeholder from the dataset is the manufacturer of the IoT devices. There are four main categories of devices identified in the area of The Hague (webcams, routers, hard drives, and home management IoT devices). Within those, there are 17 different manufacturers found. Similar types of devices from the same manufacturers show up in the data (see Appendix B: Device findings from the network scan data). This can also be caused by a data bias (as described in chapter 5).

Webcams

Within the type of webcams, there are seven different brands found. These occur a similar number of times. There is a distinction to be made between consumer-focused brands and business-focused brands. For all brands found between the webcam manufacturers, a research and development department is present at the company, and the main selling point for these webcams is safety and security. Some consumer-focused brands sell cameras aimed at households, indoor and outdoor.

Routers

When it comes to routers identified within the dataset, there are seven router brands found. Two of these brands seem to be overrepresented in the data (see Appendix B: Device findings from the network scan data). The possible explanation for this is twofold: The data selection bias created by deciding what devices to identify within all IP addresses is focused on this specific brand, which creates the overrepresentation of this brand within the data. Another aspect of this overrepresentation is the prescription of a router by an ISP. This would mean a specific ISP also has more customers using this specific router. This seems to be the case (see 6.2. Internet service providers).

Hard drives

The hard drives identified are disk stations from a single manufacturer, with the ability to be accessed through the internet. The same manufacturer is responsible for the software and ensuring safe access to the hard drive. Internet access is the main selling point of these devices.

Household IoT

The smart lights and energy monitoring devices have been grouped under 'household IoT'. The smart lights are from a single brand as well as the energy monitoring web interfaces. Important to note that the energy monitoring brand is not well known, while the lighting brand is an expert in lighting, focusing on home appliances for consumers. This shows that unknown and known brands both showcase publically accessible and vulnerable IoT devices.

Consumers tend to trust manufacturers (Emami-Naeini et al., 2019), thinking a device is secure by design if they can buy it from the store. Consumer-focused brands should be aware of this, considering that most consumers lack the technical know-how to configure or handle IoT technology like a webcam properly. On a similar account, business-focused manufacturers advertise their security technology for businesses that need it. With 'security' being your main selling point, such businesses as customers trust the webcams you sell are safe. This creates a false sense of security for consumers (Levy-Bencheton, 2018) since the wrong configuration or not following guidelines set by the manufacturer will still result in a vulnerable device, even though manufacturers implemented security measures. The security issues that result from mishandling or misconfiguration of a device are then also put in the hands of a manufacturer since users' expect a device to be safe when bought and installed (Emami-Naeini et al., 2019).

This creates a paradox that a manufacturer implements security features to make a device safer and not be responsible for vulnerabilities, which results in a user misconfiguration of the device making it more vulnerable. This, however, means devices should be made more secure by design (Melzer et al., 2020). This makes these manufacturers of IoT devices responsible as one of the main stakeholders to design and implement governance options.

6.1.2. Internet Service Providers

For every IoT device, there is a corresponding IP address that belongs to this device. To connect to the internet, an internet service provider supplies an IP address to the device, which then is able to connect to the internet. Every IoT device has a corresponding IP address belonging to the web interface and to the device itself. This address belongs to the internet service provider that owns that IP address, and therefore the ISP provided the infrastructures for the internet.

As shown in chapter 5 (5.3.4. the networks of devices: table 5.7.) 79% (151) of the devices (191) are found in consumer ISP networks, and 15% (29) of the devices are found in business ISP networks. This means a total of 180 (94%) out of the 191 identified devices are found on ISP networks. The remaining 6% are either found in business networks, or unclear, and therefore the choice is made to focus on ISPs. There are eight different ISPs identified as the provider of the networks for the devices found (see Appendix C: Findings on ISPs and device types.). These involve different sized ISPs targeted towards consumers and but also business focused ISPs.

The large-sized ISPs have a large number of customers. These ISPs are well known and have their own R&D as well as security department. The large customer base is also a possible explanation for more IoT devices found at these providers. These are primarily all-around, meaning they serve businesses and individual customers. However, the focus of the large-sized ISPs predominantly lies on consumers. Most business-focused ISPs found are relatively small compared to large-sized ISPs. They are lesser-known to the general public and therefore also have a smaller customer base.

The takeaway from this is that providers focus on service and security for their customers. Most providers make a selling point out of a decent and safe network for their customers. The different customers and sizes these providers have do not seem to make a difference in terms of vulnerabilities since similar devices with similar vulnerabilities are found at all these different ISPs. This falls in line with findings from Van Eeten et al. (2010) that also found that the size of an ISP does not mean an ISP is more secure.

The role of ISPs

Internet service providers have roles in the prevention, detection, and remediation of IoT device security issues. From a customer's perspective, the internet service provider is trusted (whether that be businesses or households) to provide safe access to the internet. As such a gatekeeper, the internet service provider must give access to the internet for their customers and do this safely. They are, according to literature, responsible for remediating security issues within their network and preventing any malicious actions that could harm other customers.
Their dual role lies in customer service and communication. An internet service provider has to communicate with these customers by providing internet services, which means giving out or prescribing equipment the customer needs to connect to the internet by giving out a specific router brand, for instance.

Vulnerabilities and ISPs

In the case of vulnerabilities in IoT devices, the ISPs have a vital role at the moment. The GDPR ensures personal data protection, which makes ISPs the stakeholder with the legal ability to reach IoT users through their IP addresses directly.
Depending on the type of vulnerability, the ISP can in theory provide support to customers to remediate issues, reach out to the manufacturer to remediate security issues or create a security solution by themselves. However, since ISPs only provide access to the internet and do not manufacture devices, you could ask whether it is the responsibility of the ISP to solve security issues. Similar devices with the same problems indicate a vulnerability at the manufacturer, while a single vulnerable webcam might indicate misconfiguration by the user. The ISPs are the only stakeholder with the ability to reach the user, and therefore form an essential stakeholder to consider during governance design.

6.2. Other main stakeholders

Other than the stakeholders found from the data, there are two other main stakeholders relevant for defining governance options to solve security issues. These will be added to the identified stakeholders from the dataset and will be addressed now.

Device users

The primary stakeholder at the endpoint of security solutions. That is, solving security issues for IoT devices revolve around the device user being 'safer'. The device users determine the success of measures taken by other stakeholders. Suppose manufacturers, for instance, completely lock their device for security reasons. In that case, you could say the device is fully secured, but if users cannot use the device anymore, this will not be very successful. It is also possible to place the responsibility of solving security issues in the hands of users if these security issues result from misconfiguring or misusing the IoT device. Device users can not create governance themselves but are the subjects. Therefore device users are an essential stakeholder to take into account when designing governance options.

The municipality

The starting point for this research is the realization of a smart city ambition by the municipality of The Hague. The acquiring of network scan data is also initialized by the municipality. As the central actor to realize this ambition, based on what the conclusions from the data (chapter 5), defining the governance options concerning securing IoT devices is important. As shown in chapter 1: local governments play an important role to realize smart cities through IoT. Therefore the municipality will be the governmental actor in the entire group of selected stakeholders.

6.3. Conclusion

Based on the empirical data, only two main categories of stakeholders are identified from the network scan data: device manufacturers and internet service providers. Within these categories, larger and smaller companies have devices with similar security vulnerabilities as their product or in their networks. Added to these stakeholders are the device users and municipality. These will form the identified stakeholders for the governance of IoT. They relate as shown in figure 6.1.

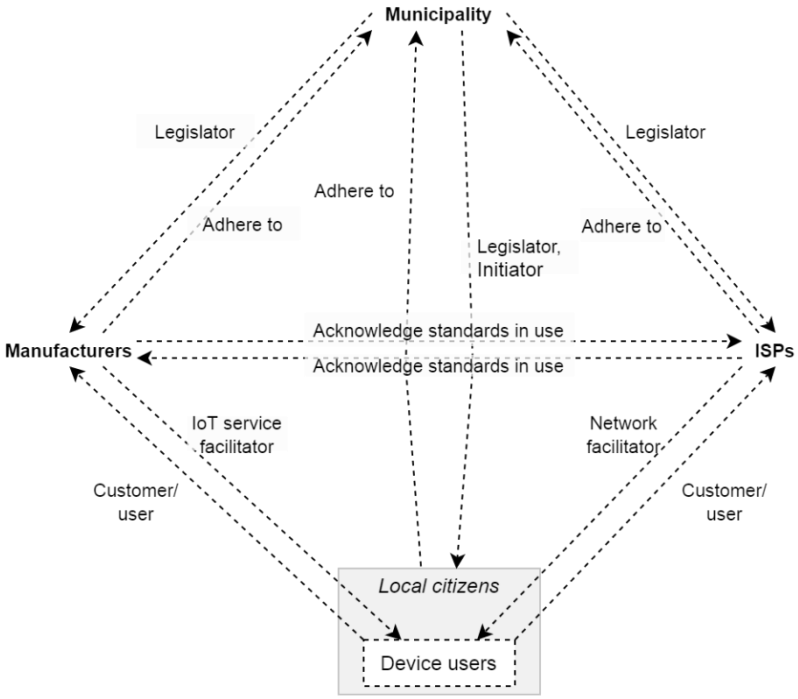

Figure 6.1 the identified stakeholders and their relations to each other.

As shown in figure 6.1, it is important to notice the difference between the groups of people a stakeholder provides a service to. Users are customers of services provided by manufacturers or ISPs. Municipalities offer services to the total local citizen population, while ISPs and device manufacturers provide their products or services to a specific group of device users. This influences the different governance options they have. It also depends on which stakeholder the responsibility lies to solve an IoT issue puts the burden of solving at another actor. There are three perspectives for this:

If IoT vulnerabilities surface due to misconfigurations, the simplest step is to make the device user responsible. Misconfigurations are a user's responsibility, so they should solve any vulnerability that surfaces through this. Relating this to the governance principles in chapter 4 indicates a tension between users expecting a device to be secure, and manufacturers not being held accountable for unsecure devices. Even though security issues can surface by design and are therefore not directly related to users, the manufacturer makes the user responsible.

Vulnerabilities can surface through network scanning, and therefore internet service providers can pinpoint vulnerable devices. In terms of governance representativeness (chapter 4), they are the right stakeholder to involve. They are also the stakeholders legally allowed to have contact information of the end-users and reach out to them. However, internet service providers are there to provide internet access. If they have to actively interact with users to solve vulnerabilities on their IoT devices, it would be resource and time-consuming. Therefore, the difficulty lies in responsibility: if vulnerabilities are found, would it be the ISP's responsibility to reach out and try to have these vulnerabilities solved actively? To design governance for ISP's accountability has to be kept in mind (chapter 4). There should be a justification for looking for vulnerabilities, and this data handling should be made transparent to the user.

The fact is that vulnerabilities, independent of how a device is configured, is part of how a device is manufactured. You could argue that a device should be 'foolproof' in the sense that, whatever a user does to

it, it should be challenging to make vulnerabilities occur. Manufacturers will have to comply with the needs of their customers (Fagan et al., 2020) to sell devices and be profitable, but also require a level of security in their devices (that in terms of governance they seem to neglect by putting the risk in user's hands). Therefore, manufacturers should actively solve these vulnerabilities when a specific device carries the same vulnerabilities with different users. This does mean a balance between security and the usability principle of governance (chapter 4). If a manufacturer were to put too much security on a device, the usability would decrease.

These three perspectives are all realistic, and therefore it seems a stakeholder should take the lead to see what should be done. For this research, this initiating stakeholder is the municipality of The Hague. The different governance principles are already highlighted within the discussed perspectives, giving a starting point to define governance options for each stakeholder. Involving these actors already indicates multistakeholder governance (chapter 4) by including public and private actors.
The options needed to solve the vulnerabilities are dependent on what described perspective is taken since it depends on which stakeholder to involve. Identification of the possible governance options with the stakeholders identified will be made in the following chapter.

7 Governance option identification

The identified stakeholders have specific means of governance available. Using different stages of an IoT device (through an IoT Use cycle) gives the possibility to assess different options structurally, and by that answering the following question: What governance options are available to the identified stakeholders?

These different governance options are either derived from literature, by looking at the current means a stakeholder has, or by thinking out of the box on what a stakeholder can do (and disregarding their current means or legal aspects). Thinking out of the box in terms of governance possibilities a stakeholder has gives the possibility to define a diverse set of options per stakeholder that might have not been described in literature yet. This does mean there are governance options which are potentially infeasible (due to a lack of legal basis, for instance) but if implemented could solve IoT vulnerabilities. This chapter is only about exploring and identifying options, while the actual feasibility and validity will be assessed in chapter 8 and 9.

7.1. IoT Use cycle

There are different intervention points during which the stakeholders could ensure safe deployment or usage of IoT. Different options can be used during various stages: buying a device needs different measures to ensure IoT security than using a device. Therefore an adaption to the IoT lifecycle described by Kotz & Peters (2017) is used to go through these stages structurally (see figure 7.1). This starts at manufacturing and ends at the disposal by the user. This also entails devices being reused (by selling it or giving it to a new user, for instance).

Within these stages, the distinction is made between three specifications for governance options: stopping a security risk from taking place (prevention; ex-ante), identifying a security risk (detection), and remediating a security risk once it has occurred (remediation; ex-post) (Kuerbis & Badiei, 2017). Using these stages does not exclude governance options from being used solely in a single stage: options are not exclusive for each stage.

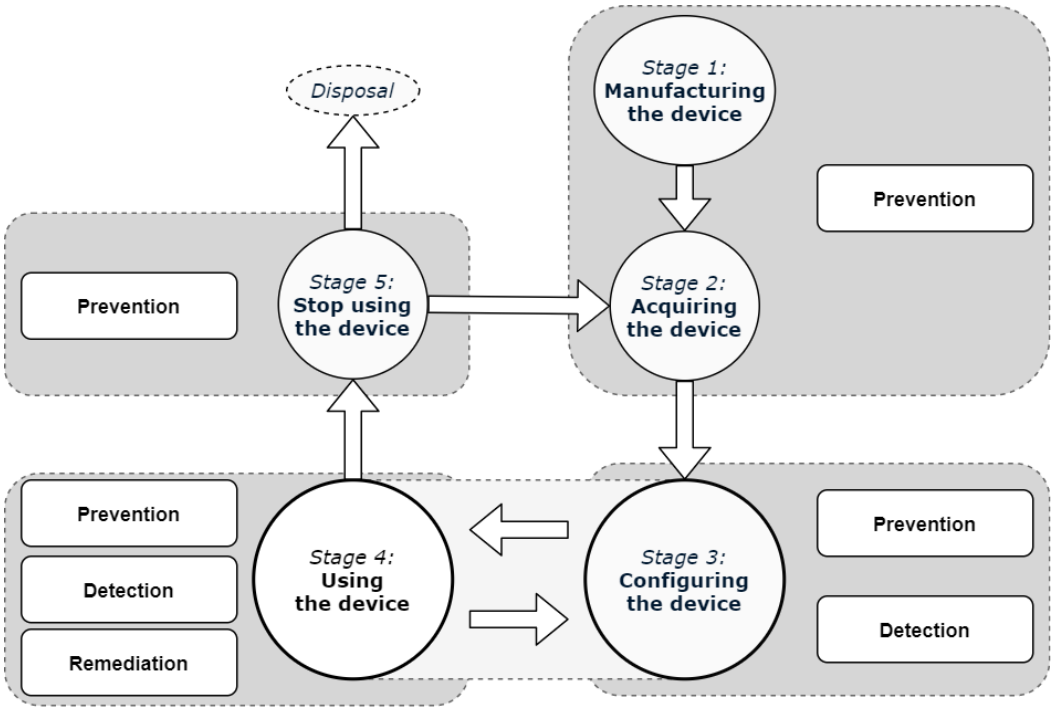

Figure 7.1 IoT use cycle, adapted from Kotz & Peters (2017). The arrows follow the cycle of an IoT device, and the boxes indicate the type of governance options (prevention, detection, remediation) in that stage.

The stages in which governance options are focused on preventing security risks from occurring:

1. Manufacturing the device:
The device should be manufactured and configured securely (Kotz & Peters, 2017) before being used. This stage mainly involves the manufacturer as a recurring stakeholder and is focused on technical device characteristics.
2. Acquiring the device:
Once a device is manufactured, users can acquire a device by buying from a vendor, directly from the manufacturer, from another user, or simply getting it for free or with a subscription (Kotz & Peters, 2017). This is the stage between a device coming from a manufacturer or previous owner and a (new) user setting up the device. There are possibilities for each stakeholder to implement governance for safer device acquisition.

3. Configuring the device:
Once a device is bought or acquired, the device owner or user has to configure it and set it up for usage. In this stage, a device has to be configured securely (Kotz & Peters, 2017). This follows from the boundaries set by a manufacturer in the manufacturing stage and originates from security-by-design (Melzer et al., 2020). Configuring the device requires knowledge about configuration since misconfiguration can be a security risk. This means this stage for a device is user-centred primarily. It focuses on governance options to prevent and detect security risks since remediation can only occur once a device is configured.

The stage that results in most governance options, focusing on prevention, detection, and remediation:
4. Using the device:
When a device is set up and configured, potential vulnerabilities (resulting from poor configuration or manufacturing) can come to light. When using a device, the security aspects are managed by the device user or owner. This means this stage for a device is user-centred primarily and focuses on governance options from all three stakeholders to prevent, detect, and remediate security risks.

5. Stop using the device:
The final stage of a device is when a user stops using the service or device itself. It is essential to notice that this includes throwing away the device, abandoning the device, not using a device anymore, or a device getting a new owner (Kotz & Peters, 2017). In that case, this stage refers back to stage 2: acquiring the device. Devices left unused can possess security issues (like outdated software, or old hardware) that new devices do not have, therefore creating security vulnerabilities that possibly already have been remediated in updated devices (Palmer, 2021). This means any governance option in this stage intends to prevent old vulnerable devices from being used, or being disposed to make sure no vulnerabilities surface.

7.1.1. Finding options

1. Manufacturing the device

With the focus on device manufacturing, these are mostly governance options targeted towards technical solutions (hard and software), with the central stakeholder being the device manufacturer. Manufacturers can implement technical security features related to hardware or software. The focus is on preventing security issues through security-by-design (Melzer et al., 2020), meaning to ensure best security practices in technology are applied, including living up to current security standards. Relating to the vulnerabilities found in chapter 5, this would for instance mean changing default passwords, secure storage of sensitive information, or automatic updates for a device (DCMS, 2018). Security-by-design is the underlying concept of every governance option for prevention by the manufacturer in this stage and the following stages.

Internet service providers do not manufacture IoT devices themselves, but they provide the infrastructure for devices to be used and facilitate some devices for users (e.g. routers). Therefore, ISPs can influence the devices used on their network, such as advising customers or allowing devices with a specific security standard onto their networks (which is only done for business IoT at the moment). This would incentivize device manufacturers to live up to the standards set by ISPs if large ISPs enforced the same standards (Stahie, 2020). If ISPs can control the devices used on their networks through permissions, there is less chance of manufacturing-related vulnerabilities being detected later on (as in the dataset of chapter 5).

In a similar role, the municipality can in theory make agreements with manufacturers or device vendors to ensure only devices are sold with a certain security standards. The flipside of this is banning unsafe devices by arguing security issues result in infringements of other laws (e.g. privacy laws). This is similar to the ban of facial recognition technology in San Francisco that resulted from privacy issues (Kate Conger et al., 2019). To apply this to IoT would require a problematization of IoT and finding legal grounds to enforce this.

This all ensures devices are as safe as possible before they are acquired by users (prevention). Potential options to ensure a secure device in the stage of manufacturing are shown in table 7.1.

Table 7.1 An overview of possible governance options during different phases for each identified stakeholder.

Prevention		
Security-by-design	1. Force two-factor authentication to log in. 2. Force mandatory password changes (from default) before usage. 3. Force mandatory password changes every set number of days. 4. Store sensitive credentials encrypted on the device or service 5. Force automatic software updates 6. Enforce the principle of least privilege: restrict user rights and services to only the functionalities they need. 7. Provide clear insights to the user how their data is being used (according to GDPR) 8. Let devices periodically send a diagnostic status report to the device manufacturer for inspection. 9. Let the device notify the device owner when the device interface is (attempted) to be accessed. 10. Set up a factory reset option that locks a device, cleans it up, brings back default values, and has a helpdesk to set up the device safely. 11. Use state of the art technology as a standard. 12. Force timely, automatic software updates. 13. Ensure the latest software version is installed before the device is being sold. 14. Design devices to operate exclusively on private networks, and if remote management is needed, have this communication encrypted. 15. Enable the function to lock the device and provide a guide to configure the device every time the device is reset safely. 16. Physically make wrong configurations through hardware impossible. 17. Enable a lock function that locks a device if a user attempts to use the device for other intended purposes. 18. Once a security issue is detected, a device gets locked and is only usable again through owner verification and guided secure setup through a helpdesk. 19. Enforce coordinated vulnerability disclosures to let vulnerabilities be researched 20. Invest in security through the acquisition of investors by promoting security aspects of your products.	Manufacturer
Steering manufacturers	21. Only allow devices that live up to specific security standards onto the network. 22. Agree with manufacturers to give out only their IoT devices to ISP customers if the manufacturer ensures specific security standards are followed.	Internet Service Provider
Steering manufacturers	23. Make agreements with specific manufacturers to only manufacture devices that live up to the current level of technology and security levels. 24. Agree with manufacturers to give out their IoT devices to citizens (as a municipality) if the manufacturer ensures specific security standards are followed. 25. Force manufacturers to make devices that follow the highest security standards. 26. Provide manufacturers with financial means to increase the level of security in their IoT devices	Municipality
Steering ISPs	27. Force ISPs to only allow devices that live up to specific security standards onto the network.	
Steering device users	28. Only allow devices to be used that live up to the current level of technology and security levels.	

2. Acquiring the device

Manufacturers can provide (potential) users with knowledge about security-related information concerning the device (Emami-Naeini et al., 2019). This could also be done through notifying customers by highlighting potential vulnerabilities on their website.

The municipality has similar options as during the manufacturing of devices. Added to this, the municipality can subsidize devices that are shown to be safe through discounts, for instance (e.g. give out gift cards to buy a Google Home speaker if that speaker is shown to be safer than other brands). Creating more awareness, considering that a study in the United Kingdom found that 40% of IT users are unaware of IoT security (BSI, 2018). The municipality can set up an IT department that actively inspects and checks IoT devices being sold to ensure they are safe. Added to this, the municipality can organize a campaign to increase awareness and inform citizens about devices and security issues (The Hague Security, 2020). All these options rely on IT knowledge to be present at the municipality (or outsourced to a third-party) and need to define what IoT standards are and what is secure.

Internet service providers could do a similar campaign since any vulnerable devices would make use of their networks. The difference between ISPs and the municipality in this sense is the target audience. While the municipality can target no specific audience unless they can acquire addresses of device users, the ISPs can in theory target their customers specifically. This indicates a similar role taken by the different stakeholders, with the ability to reach a different group of people. ISPs at the moment also advise on using only certified IoT devices in business IoT, for which they also have a dedicated helpdesk. Applying this to consumers would result in fewer vulnerabilities as found in the dataset in chapter 5. This is still only just advice since there are no legal grounds that force customers.

The governance options possible are shown in table 7.2.

Table 7.2 An overview of possible governance options during different phases for each identified stakeholder.

Prevention		
Informing device users	29. Add a security label or security information to the device packaging to inform users about potential vulnerabilities before buying. 30. Place a notification of potential vulnerabilities or misconfigurations on the device manufacturer website. 31. Set up a helpdesk to give users the ability to call if users believe their (new) device might be at risk. 32. Give the warranty to users to swap 'infected' devices with new devices (through vendors or the manufacturer)	Manufacturer
Steering manufacturers	33. Make agreements with specific manufacturers to only manufacture devices that live up to the current level of technology and security levels. 34. Provide manufacturers with financial compensation to sell a more secure device for lower prices and less secure devices for higher prices. 35. Require manufacturers to add a security label or security information to the device to inform users about potential vulnerabilities before buying.	Municipality
Policing IoT	36. Setup an IT department that inspects and checks devices being sold.	
Informing device users	37. Set up a campaign to advise users on what makes a safe device and what to look for when buying an IoT device. 38. Setup a security label as a municipality that indicates how secure a device is. 39. Set up a website where customers can check how secure a device is before buying/acquiring it.	
Steering device users	40. Only allow devices to be used that live up to the current level of technology and security levels. 41. Force device vendors to only sell devices that live up to a specific security standard. 42. Provide device vendors with financial compensation to sell a more secure device for lower prices and less secure devices for higher prices. 43. Provide users with discounts for specific devices that are the safest options.	
Steering device users	44. Give out devices to ISP customers that the ISP approves as being secure. 45. Do not allow other devices than the devices approved or supplied by the ISP onto the network.	Internet Service Provider
Informing device users	46. Setup a security label as ISP that indicate how secure a device is. 47. Set up a website where customers can check how secure a device is before buying/acquiring it. 48. Provide advice on using certified devices to customers to ensure security.	

3. Configuring the device

In the previous stages the governance options are focused on implementing technical interventions and informing users before buying a device to prevent vulnerabilities. During the stage of configuring the device users start to configure and actually use the device. Therefore, automatic software updates on a device would take away responsibilities from the user and prevent exploitation through software vulnerabilities. The same goes for a factory reset option before configuring a device that locks a device, cleans it up, brings back default values, and has a helpdesk to set up the device safely. After configuring, the ability to detect vulnerabilities (resulting from device configuration) can be implemented through a diagnostic status report is send to the device manufacturer to find out about any security issues that might surface. For similar reasons, a helpdesk with device knowledge can be set up by the manufacturer to allow users to call if they believe their device might be at risk. This can also be forced by legally having manufacturers provide a level of support or updates for x amount of time.

To inform users about vulnerabilities of the device they are about to use, a manufacturer can notify users of potential vulnerabilities or misconfigurations on the primary device interface or webpage. This could also include guidelines on how to configure the specific device safely. This would rely on users to have technical skills and knowledge to solve security issues.

For ISP's safe configuration of a device will result in secure network use and fewer vulnerabilities that can escalate and are detected through network scanning or devices that need to be remediated. Therefore setting up a helpdesk that knows how to help users set up their IoT device safely could be beneficial. ISPs can also force users to use a VPN connection by providing this, ensuring IoT devices are undetectable or accessible from other locations than the user's home address. This would, in a way, force secure-by-design network usage from the ISP's perspective.

ISPs can scan networks for vulnerable or misconfigured IoT devices, just like the data of Cybersprint, to detect vulnerabilities, after which they hypothetically can contact people based on that IP address to notify them about security risks found (Melzer et al., 2020). This is an essential role that will further be addressed in the following stage: using the device.

The municipality has been more of a bystander than an active participant in this process for the options. They can only inform (potential) device users by reaching out to their citizens (by sending out letters, for instance) to inform them about IoT devices and security practices, organizing a campaign with the same goal, or setting up an IoT helpdesk themselves that specializes in a secure configuration. All these options would, however, rely on technical knowledge by the municipality.
The options that result from the possibilities these stakeholders have in this stage are shown in table 7.3.

Table 7.3 An overview of possible governance options during different phases for each identified stakeholder.

Prevention		
Informing device users	49. Setup a helpdesk to help users set up their device 50. Force users to call a helpdesk before being able to set up their device safely 51. Require the device to be configured by an expert provided by the manufacturer.	Manufacturer
Informing device users	52. Setup a helpdesk to help users set up their device	Internet Service Provider
Steering device users	53. Force users to call a helpdesk before being able to set up their device safely. 54. Require the device to be configured by an expert provided by the Internet Service Provider.	
Informing device users	55. Setup a helpdesk to help users set up their device 56. Set up a campaign to inform users on how to configure their device and what to keep in mind in terms of security. 57. Send out a letter to every citizen informing them of IoT safety and configuration.	Municipality
Steering device users	58. Require the device to be configured by an expert provided by the municipality.	
Policing IoT	59. Give out certificates that officially state a device is configured securely.	
Detection		
Informing device users	60. Scan networks for vulnerable or misconfigured IoT devices and reach out to device owners to notify them about security risks found. 61. Go door-to-door at ISP customers to check whether there are IoT devices misconfigured	Internet Service Provider
Policing IoT	62. Go door-to-door at ISP customers to check whether IoT devices are misconfigured and solve issues on the spot. 63. Only allow IoT devices to be used through a VPN tunnel.	
Informing device users	64. Inform citizens in general about potential misconfigured IoT devices they might own and have them contact the manufacturer or vendor. 65. Go door-to-door to check whether there are IoT devices misconfigured	Municipality
Policing IoT	66. Go door-to-door to check whether there are IoT devices misconfigured and solve issues on the spot.	

4. Using the device

The options device manufacturers have relate to security-by-design and are primarily addressed in the previous stages. The technical features that secure this stage of using an IoT device result from the options defined in the manufacturing stage. The same goes for the municipality. The options discussed in previous stages are not exclusive and still apply to using the IoT device.

In keeping IoT devices secure while being used, according to literature, the ISPs have an essential role at the moment. Their tasks consist of two parts (Hay Newman, 2016): Providing the means to detect IoT-related security issues within their networks and contacting these users directly (Melzer et al., 2020). As concluded in chapter 5, ISPs are currently the only link between detecting vulnerable devices and being able to reach users. ISPs can keep a check on telemetry data (usage and measurements) within their networks (DCMS, 2018), resulting in essential options to reach device owners or users. The options to reach users on their device vulnerabilities should then be incorporated in the ISP's network use policies, like using a network to spread copyrighted material in the United States (United States Government, 1998), explicitly applied to IoT vulnerabilities.

The options an ISP has to solve vulnerabilities after reaching out to the user could entail only notifying a user, quarantining the user's device, or also help the user in solving the security issue before taking the device out of quarantine (Cetin, Ganan, Altena, Kasama, et al., 2019). Because no legislator has any legal grounds to force a 'clean up' once vulnerable devices are detected, you could also suggest having ISPs voluntarily solve vulnerabilities in user devices like they remediate and clean up their networks at the moment (M. Van Eeten, 2017).

The options that result from the possibilities these stakeholders have in this stage are shown in table 7.4.

Table 7.4 An overview of possible governance options during different phases for each identified stakeholder.

Prevention		
Informing device users	67. Place a notification of potential vulnerabilities or misconfigurations on the device manufacturer website. 68. Place a notification of potential vulnerabilities or misconfigurations on the primary device interface or webpage.	Manufacturer
Informing device users	69. Set up a campaign that shows people how to use an IoT device safely. 70. Send out a letter to every citizen, informing them of IoT safety and configuration.	Municipality
Informing device users	71. Setup a campaign that informs customers how to use an IoT device safely.	Internet Service Provider
Detection		
Informing device owners	72. Scan networks for vulnerable or misconfigured IoT devices and reach out to device owners to notify them about security risks found. 73. Set up a helpdesk to give users the ability to call if they believe their device might be at risk. 74. Go door-to-door at ISP customers to check whether there are IoT devices used and configured insecurely.	Internet Service Provider
Steering manufacturers	75. Use a 'three strikes, and you are out' principle, following from the data in networks. If a device manufacturer shows up repeatedly, the manufacturer will be banned from the networks after three 'strikes'.	
Informing device users	76. Inform citizens in general about potential misconfigured IoT devices they might own and have them contact the manufacturer or vendor. 77. Go door-to-door to check whether there are IoT devices misconfigured	Municipality
Steering ISPs	78. Have public networks scanned and find the ISPs belonging to vulnerable devices: then force these ISPs to contact the device owners belonging to these devices.	
Remediation		
Informing device users	79. Set up a helpdesk that provides users with a manual or guidelines on how to remediate the security issues found on their device. 80. Provide users with a manual or guidelines on how to remediate the security issues found on their device. 81. Place an up to date guide on how to remediate the security issues found on the manufacturer's device.	Manufacturer
Informing device users	82. Provide users with a manual or guidelines on how to remediate the security issues found on their device.	Internet Service Provider
Policing IoT	83. Quarantine a user device when a security issue is found, only to be taken out of quarantine once the security issue is remediated. 84. Reach out to device owners through a helpdesk, and fix the security risk together with or for the device owner.	
Steering ISPs	85. Pressure ISPs to do a device cleanup in terms of vulnerabilities 86. Have public networks scanned and find the ISPs belonging to vulnerable devices: then force these ISPs to contact the device owners belonging to these devices.	Municipality

5. Stop using the device

Manufacturers should keep in mind measures to dispose of a device safely (Fagan et al., 2020), relating to security-by-design (Melzer et al., 2020). Related to device disposal functionalities to be added are a reset of password or login credentials or even the complete IoT device after not being active for an x amount of days.

For this stage, the ISPs and municipality can again take a similar role, just like in previous stages for setting up a campaign to inform users. In this stage, they both can set up a collection point for users to dispose of their 'old' IoT device. This would benefit the ISPs since 'older' devices carry 'older' security practices that are mostly more vulnerable and desirable to take of your network (Hay Newman, 2021). Vulnerabilities found in chapter 5 might not be noticeable once a device is unplugged or not used, but once used again, these same vulnerabilities will surface. Again the difference between the ISPs and municipality in this approach is reaching a specified group of users for the ISP. In contrast, the municipality can only target the entire population of the municipality without targeting specific device users.

The governance options to ensure a safe IoT device in this stage are shown in table 7.5.

Table 7.5 An overview of possible governance options during different phases for each identified stakeholder.

Prevention		
Security-by-design	87. Enable devices to reset themselves if the service or device is not used in an x number of days. 88. Reset user passwords if the service or device has not been used in an x number of days.	Manufacturer
Informing device users	89. Buy old/not used IoT devices from users. 90. Give discounts on new IoT devices when users hand in old devices.	
Steering device users	91. Setup a collection point for customers to dispose of their IoT devices to ensure safe disposal/reset of these devices. 92. Buy old/not used IoT devices from users. 93. Give discounts on new IoT devices when users hand in old devices.	Internet Service Provider
Policing IoT	94. Give out certificates with a date belonging to a device that state the level of security a device has at that moment, ensuring only a specified level of security is allowed and the certificate is up to date before given to new users.	
Steering Device users	95. Setup a collection point for customers to dispose of their IoT devices to ensure safe disposal/reset of these devices. 96. Buy old/not used IoT devices from users. 97. Give discounts on new IoT devices when users hand in old devices. 98. Go door-to-door and force users to upgrade their device to a new model. 99. Setup a device selling website the lets users give their IoT device, have it updated and brought to the highest security standards, and then sold to other users.	Municipality
Policing IoT	100. Give out certificates with a date belonging to a device that state the level of security a device has at that moment, ensuring only a specified level of security is allowed and the certificate is up to date before given to new users.	

7.2. Causal relationships

The options do not exclude each other. This means option A does not exclude option B from being implemented (e.g. implementing password changes does not exclude the option also to set up a collection point for old devices). However, a distinction can be made between governance options that can simultaneously be done and options that result from failing previous options. Some stages precede each other from the IoT use cycle, which means successful security measures in a previous stage will result in less need for more governance options in the following stage. Also, successful implementation of prevention options will lead to less need for detection options, and successful implementation of detection options will lead to less need for remediation. To illustrate this, the actors in the chain from manufacturer to user are shown in figure 7.2.

Looking at responsibilities and possible governance options, you could argue that if a device is 100% secure by design, there is no need for other stakeholders to implement governance options (while still requiring to dispose a device safely). When a device can not be entirely secure when it comes from the manufacturer, the responsibility shifts to the following stakeholders in the chain. The municipality is not shown in the chain in figure 7.2, as they can implement governance measures to influence other stakeholders. The takeaway here is that deploying all options at the same time by all actors would be inefficient. If prevention methods at a previous stakeholder succeed, there would be less need for the following stakeholder to implement prevention/detection/remediation options.

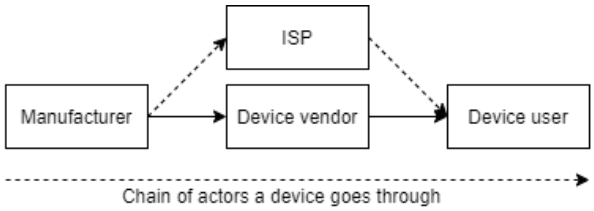

Figure 7.2 A general overview of actors that handle a device before reaching a user.

There are similar types of options per stakeholder. ISPs and the municipality can both implement options that steer device users or manufacturers. They also both can deploy options categorized as policing of IoT. These options are also not exclusively used by a single stakeholder, and collaborations will later be discussed during validation (chapter 8) and synthesis (chapter 9). The difference for each stakeholder is the means they have and the group of people they can influence (as discussed in previous paragraphs).

In figure 7.3, a causal diagram is shown with the main governance categories per stakeholder. A green arrow means: if A increases, B also increases (and vice versa). A red arrow means: if A increases, B decreases (and vice versa). This figure shows that ISPs and the municipality have similar options in terms of prevention that trace back to steering manufacturers to implement more security-by-design. The options that the ISPs and municipality have when it comes to detection and remediation result from a lack of prevention options from the manufacturer. Figure 7.3 indicates that, by failure to implement the successful options in a previous stage, the stakeholders in the next stage are tasked with solving security vulnerabilities. Especially starting at prevention and having manufacturers involved would result in less need for detection and remediation efforts by ISPs and the municipality, resulting in less governance options to implement.

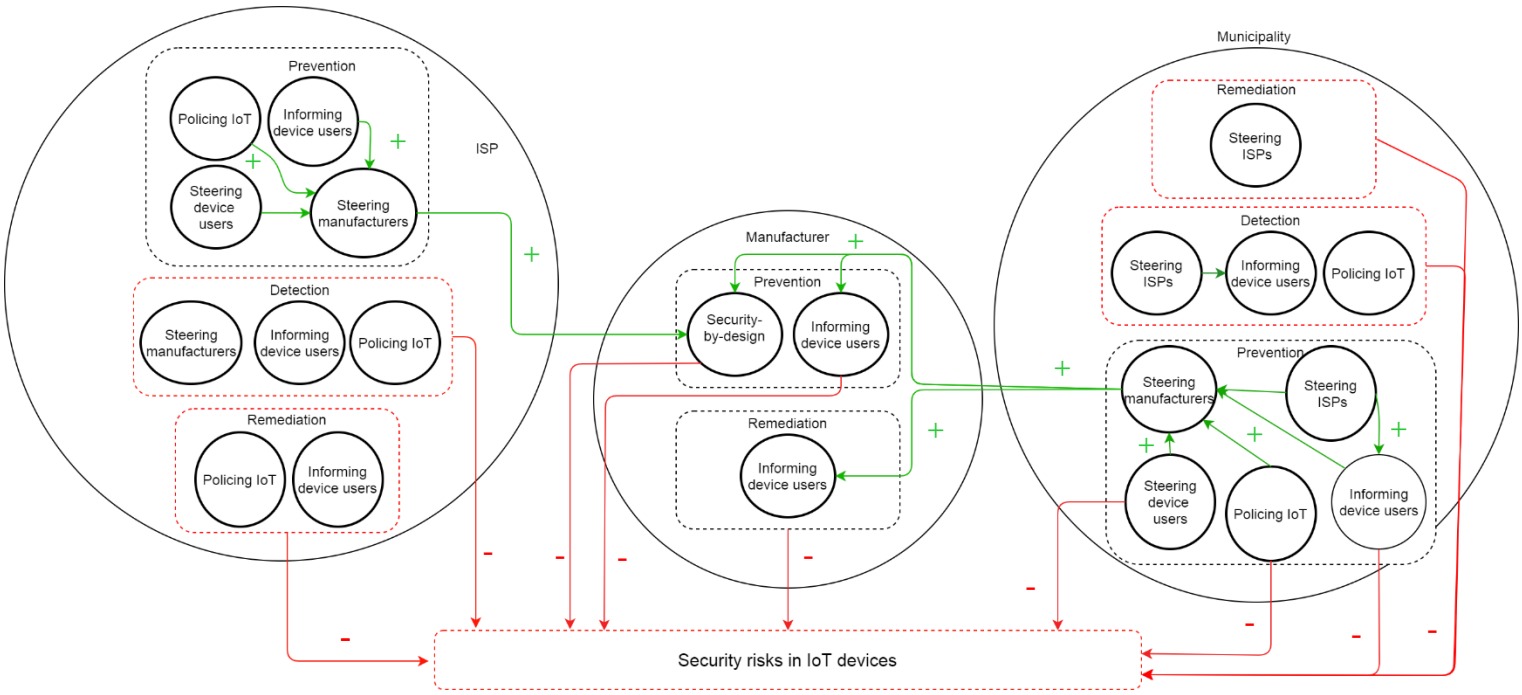

Figure 7.3 Causal relations between the different types of governance options defined.

Power-interest grid

Based on the power and interest a stakeholder has in solving security issues in IoT devices, a power interest grid is made (figure 7.4). The grid shows all identified stakeholders have a relatively high interest in solving security issues since more security always seems better. However, it depends on whether you look at prevention, detection, and remediation when it comes to actual power to implement changes.

In the prevention stage, the key player seems to be manufacturers since they have the most power through security-by-design (key player) but seem less interested since they have to be incentivized to look into security measures. In detection and remediation, this power shifts to ISPs since after configuration and usage of IoT devices ISPs can actively look for insecure devices in their networks. During prevention, ISPs have less power since they can only control what is in their networks. The municipality has power during all three phases, but this power mainly comes from influencing or steering other stakeholders into implementing changes or acting (see figure 7.3 causal relations). Therefore the interest is high, but the actual power is lower than the manufacturer in prevention and manufacturers and ISPs for detection and remediation.

Device users are the main subjects, and it could be said that most device users have a high interest in having a secure IoT device. Still, the options they have to achieve this rely on the information and options given by the other actors involved. Therefore the device user's interest is high, but their power is less than the other stakeholders.

Power-interest grid during the prevention-phase:

Power-interest grid during the detection and remediation phase:

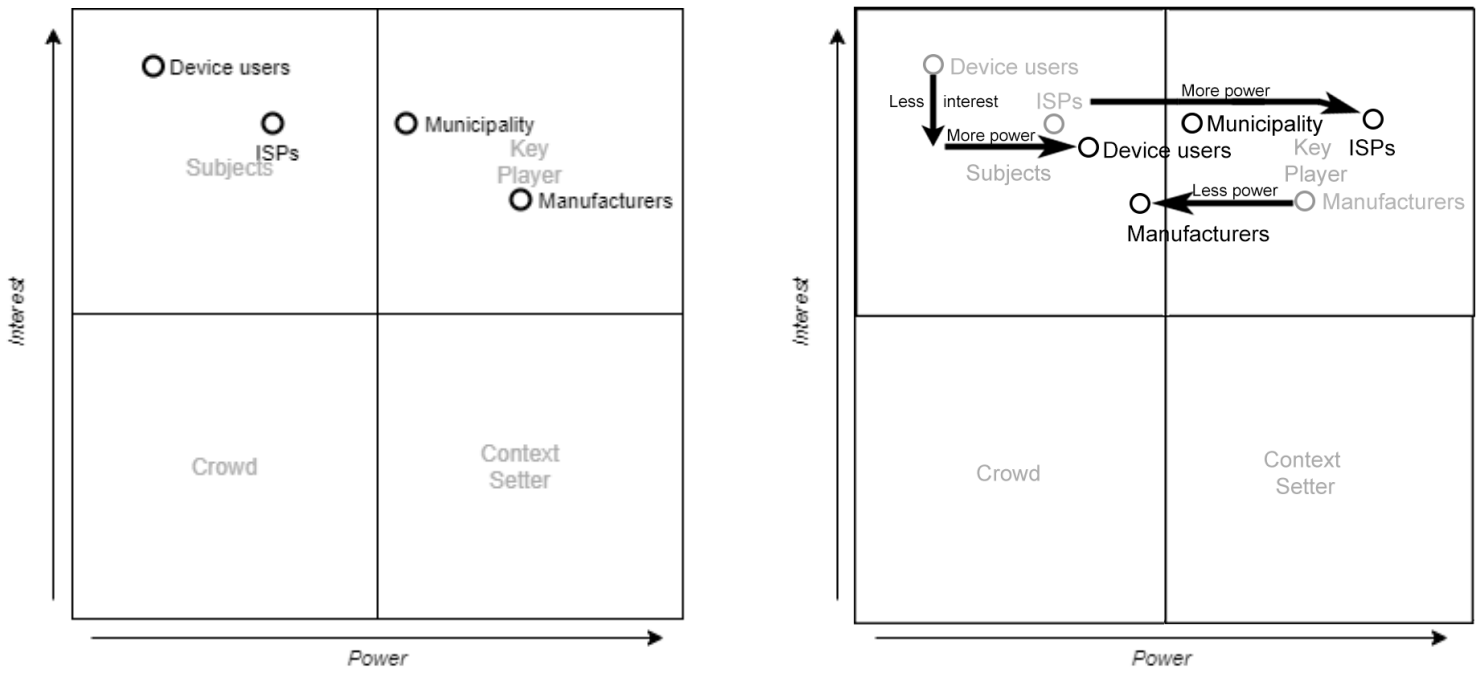

Figure 7.4 Power-interest grids (Bryson, 2007) during the prevention, detection, and remediation phase. The arrows indicate the shifts in power/interest between the different stages.

7.3. Conclusion

Based on the collection of governance options (see Appendix G: Collection of options) by the identified stakeholders, there are overlapping categorizations that show the groups of governance options possible for each stakeholder (see table 7.6). With this the research question of what governance options are available to the identified stakeholders, is answered.

Table 7.6. An overview of the defined governance options as different categories of options, with each corresponding stakeholder.

	Security-by-design	*Steering manufacturers*	*Steering device users*	*Informing device users*	*Steering ISPs*	*Policing IoT*	**Total**
Municipality	-	23-26, 33-35	28, 40-43, 58, 95-99	37-39, 55-57, 64, 65, 69, 70, 76, 77	27, 77, 85, 86	36, 59, 66, 100	38
Manufacturers	1-20, 87, 88	-	-	29-32, 49, 67, 50,51, 68, 79-81, 89, 90	-	-	36
ISPs	-	21, 22, 75	44, 45, 53, 54, 91-93	46, 47, 48, 52, 60, 61, 71, 72-74, 82	-	62, 63, 83, 84, 94	26
Total	22	10	22	33	4	9	100

Security in IoT devices start at manufacturing, and choices made in this stage result in a safer device in the following stages. The primary stakeholder in this stage is the device manufacturer. Most governance options proposed originate from the general idea of security-by-design. This technically scoped governance essentially comes down to securing a device through features to ensure the chance of vulnerabilities or misconfigurations occurring is low. This still puts some responsibility on device users since no device can be made entirely safe or without risk. However, by making a device more secure by design, governance options in a later stage do not need to be implemented. Another set of governance options for manufacturers is informing the device users through technical features and information provided through packaging or the device website.

The different options that the municipality has come from the desire to innovate and become a smart city, and therefore be involved in the security of IoT devices. This results in governance options that have to incentivize or force other stakeholders into using some standard (e.g. making agreements with vendors to only sell devices living up to specific standards) or performing a duty (e.g. forcing ISPs to reach out to vulnerable device owners). The other options the municipality has to inform and make the general public aware of security vulnerabilities and configurations of IoT devices. The municipality is more like a bystander in raising awareness through these options than actually preventing IoT device vulnerabilities as an active participant. The internet service providers have fewer governance options but play an essential role in reaching IoT device users at the moment. They are legally allowed to contact users through IP addresses and can find vulnerabilities through scanning their networks. Their remediation options for infected devices have already proven themselves to be effective (Cetin, Ganan, Altena, Tajalizadehkhoob, et al., 2019) and could be applied to vulnerable devices as well. Added to this, they also have options to inform their customers about vulnerabilities and control what devices are allowed to be used on their networks.

The defined options seem possible and are based on the intervention points found at the stage of manufacturing a device, acquiring a device, configuring a device, using a device, and stop using a device. As found in literature in chapter 4, the preference would be not to put all responsibilities in the hands of device users but rely on stakeholders higher up in the chain to ensure more device safety. Therefore the focus of governance options for new devices should be on the prevention phase. Devices already in use rely more on detecting issues and remediation and therefore targeted more towards device users.

However, some barriers stop the defined options from being put to practice, as indicated by the power interest grid: different stakeholders have different power and changing interest. This goes back to incentives for these stakeholders to act. Therefore the real-life feasibility of these options will be addressed. The barriers that stop these options from being realized will be discussed in the next chapter through option validation.

8 Option validation

The collection of governance options from chapter 7 have to be validated to see their feasibility and where the boundaries for implementation lie. This results in answering the following sub-question: How do the involved stakeholders view the identified governance options? The role and perceptions of manufacturers, ISPs, and the municipality (Identified stakeholders; chapter 6) have to be taken into account to find out if the identified IoT issues are also concerns of these stakeholders. Who should be in charge or take the lead in implementing the defined governance options, the feasibility of the identified governance options, and the boundaries or conditions needed to ensure implementation of the identified governance options will described in this chapter.

8.1. Semi-structured stakeholder interviews

The strategy for validation is through data source triangulation to gain different perspectives and therefore validate the information (Carter et al., 2014). The data to do this is provided through interviewing identified stakeholders (chapter 6) to create a broader understanding of the defined options. Using semi-structured interviews to find out about an interviewee's perspective, ensuring an informed conversation that provides discourse on the subject of this research (Qu & Dumay, 2011). The participants are three big-sized ISPs, also found in the network scan data, and the municipality (Table 8.1). Two manufacturers were also reached out to, but they did not respond. To validate the manufacturer's options, desk research with literature and information stated by the ISPs and municipality will be used as a source.

Table 8.1 An overview of stakeholder participants interviewed, and participant number for referencing.

Stakeholder	Participant
ISP A	P1
ISP B	P2
ISP C	P3
The municipality	P4

About the semi-structured interviews

By using an interview protocol (see Appendix E: Interview protocol) informed questions can be used as probes to elicit an elaborate response (Qu & Dumay, 2011), while also giving the ability to talk more freely about the subject. The interviewees were a government official and three ISP representatives affiliated with IoT and security within the stakeholder they represent. The interviewees were provided with an information sheet on the research (see Appendix D: Information sheet) before the interviews were conducted. Interviewees remain anonymous, and only the type of stakeholder (ISP or municipality) they represent will be referenced (see table 8.1). Anonymization and using semi-structured interviews ensured the interviewees could give their expert opinion without being personally addressed.

The interviews are used to determine the role of the stakeholder the interviewee represents and their view on the identified information from the dataset in chapter 5 (devices and vulnerabilities). To find out about the interviewed stakeholder's perspective on the identified problem, and what role the other stakeholders (other than the interviewee) should have in solving IoT vulnerabilities (according to the interviewee). This means ISPs were asked about their role, and what they think manufacturers and/or municipalities (or possibly governments) should do. The municipality was asked about their role, and what ISPs or manufactures should do.

After finding out the perspective and perceived role of the interviewee, the governance options of chapter 7 are used as probes for the conversation, to validate relevant options for each interviewed stakeholder and to find possibilities to make the governance options happen. This does not mean every individual governance option defined in chapter 7 was discussed, but some categories of the options for each stakeholder was brought up in the conversation. Based on the information a stakeholder provided (see Appendix F: Short interview report) on their role and response to the governance option it was determined if this would also rule out other options from being implemented as well. For instance, if ISPs do not want to send out a letter to every customer if they consider it not their role to play, then they would also not want to go door-to-door at every customer.

How these interviews are used

First, the perspective of each stakeholder (manufacturers, ISPs, the municipality) in solving IoT vulnerabilities will be discussed in paragraph 8.1.1., referring to the conducted interviews as a source of information. The following aspects will be addressed per stakeholders:

- *Role and perspective on the data findings*: Understanding if the stakeholder has concerns about the number of IoT devices and security issues found from the data or if a stakeholder does not perceive this as a problem (or at least not as something they should fix). The interviewees were asked what they thought about the findings from the dataset, and if something should be done.

- *The roles and responsibilities of other involved stakeholders*: Knowing at what point vulnerabilities should be fixed according to the interviewed stakeholder, and who should fix it according to them. Is a single stakeholder responsible, or should more stakeholders be involved and have a say in this as well? By asking the ISPs and municipality who they think should do something will give an insight into their perspective on the problem, and who they think is responsible.

For the manufacturer's perspective, literature and interviews with the ISPs and municipality will be used as sources since no manufacturer was interviewed. The different perspectives of the manufacturers, ISPs, municipality will be described in paragraph 8.1.1. Then in paragraph 8.2. the different (categories of) governance options proposed in chapter 7 will be discussed, and quotes provided by the stakeholder interviews will be referenced to address why these options work or not work. Based on this analysis for each category of options, the information of paragraph 8.1.1. and 8.2. is combined to find certain conditions and boundaries for the discussed governance options of chapter 7 in paragraph 8.3.

8.1.1. The perspective of the three different stakeholders

Using the conducted interviews and literature as a source the perspective of manufacturers, ISPs, and the municipality on the identified problem (vulnerabilities found in IoT devices) will be discussed. From this not only the perceived roles for each stakeholder will be more clear, but also the roles each individual stakeholder believes the other involved stakeholders should play.

Manufacturers

According to literature it seems like manufacturers acknowledge that they are responsible for some level of security in their devices, and they do seem to recognize the problem. However, years of proposing standards to hold manufacturers reliable for poor device security with little results indicate that no manufacturer feels directly responsible for security-related device issues (Herr et al., 2021). Liability is a significant issue, and it's unclear who should be liable in case of an IoT security vulnerability (DeNardis, 2020). This comes from the fact that, due to a lack of standards and clear agreements, the responsibility of fixing an IoT issue can be placed in the hands of the users through terms and conditions. Misconfigurations, not updating software, or using default passwords are all on the user's side. Even though manufacturers advocate for security by design and security by default (Levy-Bencheton, 2018), in practice device manufacturers want to sell devices, and their role in terms of product liability is known to be unclear (Grapperhaus et al., 2018). Therefore it seems

that once a device is sold, device manufacturers take their hands off and feel less responsible for it. As an internet service provider said: *"As long as devices sell, manufacturers do not feel the need to improve security*" (P2).

A similar conclusion is made by another internet service provider (P3), adding a specification of manufacturers involved: *"the causes for the IoT problems that now exist are caused by manufacturers",* and he gives three reasons for this:
First*, "there are manufacturers that cannot help it. They produce a fridge and are good at their job. Suddenly, they have to add an IoT element, causing security issues"* (P3).
The second reason is "*manufacturers that know things about security and try but are still not good at it. This puts a responsibility on the user: manufacturers try and add security measures, but the user still has to use these wisely"* (P3).
The last reason stated is "*the manufacturer that knows about security issues but does not care: as long as devices are sold"* (P3). All together this indicates manufacturers from their perspective not feel responsible for device vulnerabilities. They feel that users are responsible, since users will buy a device even if it is not secure.

Internet Service Providers

In general, ISPs recognize the problem of vulnerable IoT devices being used (Stahie, 2020), saying *"it is a problem that needs fixing"* (P3). The ISPs can, in theory, act as a control point to keep the networks safe (M. J. Van Eeten et al., 2010), but their *"(our) exact role is not to solve IoT vulnerabilities, only act as a facilitator*" (P1). Risks that customers create for themselves (by setting up unsafe IoT devices, for example) and how a customer uses this network is the customer's responsibility (P2). *"Only once there is unusual network traffic ISPs will investigate and notify a customer in general terms to look at their devices. They are not at blame, but only once a device is infected and acting on its own we have to act on it." (P3).*
In terms of responsibility, this internet service provider also states that finding solutions for the vulnerabilities identified in the network scan data primarily lies with manufacturers and users (P2). *"It would be weird if you want to use a device yourself, and I as ISP start to interfere with it. You would not want that as a user and as ISP" (*P3), giving the disclaimer: *"as long as you act according to the network agreement, meaning no unusual or disproportional network usage"…" every risk involved is the responsibility of the user."*

Legally internet service providers are only required to act on vulnerabilities if a customer opts in and wants to be notified or helped, or when the vulnerability has escalated and harms the reputation of the ISP as a whole through malicious activity (e.g. botnets) (P2). They have no role to proactively look for vulnerabilities that are (for now) only risks for the user since these are not affecting the network (yet). As an ISP said: *"there are laws you have to follow as ISP, and these laws are not specified for third parties like Shodan, for instance. Third parties can scan, have some shadow administration next to it, and say: you on IP address x have a problem."* (P2).

There is a considerable risk in terms of violating the law since *"scanning all IPv4 space, scanning port numbers, and identifying software and operating systems comes close to the start of hacking a device. Putting a CVE database next to it, and you know how to get in"… "I would think twice before actively doing this."* (P3). For every action an ISP does that looks into a customer's network (use), they have to ensure through the legal department that *"it's according to the law, and cannot be seen as deep packet inspection"* (P2).

In terms of governance options, this automatically excludes policing IoT (option 62, 83, 84, 94) from being realized, since going door-to-door or help customers to configure and secure a device is legally as well as practically not executable, nor do ISPs want to (P1/P2). Also, ISPs are not insured to offer this kind of service: *"Detecting a device and saying it probably has software version x, and therefore a customer needs to do patch y. This is so uncertain, we would be in headlines if for 10% of the people these fixes do not work or make the problem worse"*(P3). This was also shown in the confidence percentages in the network scan data, with no absolute certainty. Adding to this point, *"if hypothetically we did something like that, we would have to physically go to a customer. Connect our own devices. Look at all packets. Get permission for deep packet inspection. Physically look for the IoT device etc. This is business that we will not do or can not do."* (P3). ISPs do not feel responsible for solving vulnerabilities that originate from further up in the chain (P1). *"Safe devices start at the manufacturer"* (P3).

The Municipality

From the network scan data, the municipality acknowledges that IoT vulnerabilities pose a problem for device users (P4*). "As a city, digital security is part of security"… "If someone in the street is being attacked, you call the police and help them. Now we know there are vulnerable people, and it feels like we should help them"* (P4). However, the municipality does not feel responsible for solving the IoT vulnerabilities*: "We (the municipality) are not responsible. In the end, it is an individual problem (at the user)"* (P4). The role they want to play is leading actor that facilitates the right conditions for other actors to get involved. This means the municipality does not feel responsible for solving these issues through their own action. The municipality wants to identify problems and then inform other actors and decide how to act (P4). Their focus lies on developing public-private partnerships to ensure different actors have a say and can share knowledge (Bruines, 2018a).

By setting up projects (like scanning their city networks through Cybersprint), the municipality wants to gain insights into IoT: *"We financed this to gain more insights and see if there is a problem"* (P4), which they do recognize. However, the goal is to *"become a frontrunner in the area of security"* (P4). Within the Netherlands, the municipality of The Hague takes the lead in smart city realization through their primary focus on safety and security (Bruines, 2018b). *"The Hague can be a pioneer as a smart city and can take that leading role"* (P3)*…." by (cooperating with) international organizations for instance"…" That's the reason why we do this: of course the city has to be safe, but the next step is to implement things nationally"…" We recognize a problem, and then, in the end, it can be taken up nationally"* (P4).

In general, the need to facilitate technology innovations is recognized. Through financial support (option 36, 42 & 34), the municipality of The Hague facilitates pilot projects, including the scanning of their networks to find IoT problems. In this sense, the municipality can learn about a problem, but the following steps to solve this problem are unclear (P4).

8.2. Options and means

The perspectives of the manufacturers, ISPs, and municipality have been described. Using this as a starting point, the different (categories of) governance options from chapter 7 will be addressed to find out if the interviewed stakeholders are able to implement these options, or find out why they are not implementing these options or able to implement these.

8.2.1. Security-by-design

The security-by-design options (22 options) are the responsibility of the manufacturer. These options are technically executable, and most are in some way put to practice in real life. However, the catch is that, considering the thousands of manufacturers worldwide, there is a difference in technical means and expertise per manufacturer. Manufacturers who know how to "produce a fridge" and have to add connectivity have a lack of knowledge (P3). The manufacturers that attempt to implement more security-by-design lack the knowledge and end up with insecure devices. Then some manufacturers knowingly cut corners in terms of security to make money: *"There is no incentive to implement more security options into a device if the customer buys this device anyway*" (P2).
Security-by-design is centred on prevention and, therefore, will take away responsibilities for vulnerability detection or remediation from ISPs or users (P2). *"The heterogeneous network of IoT devices causes that there are no general solutions that apply to all devices."* (P3). As shown by the role of manufacturers, there is either *"a lack of knowledge"* (P3) or no economic incentives for manufactures to implement security measures.

To make it work

Forcing more security measures in devices (option 21, 22, 75) through legislation is a viable option. *"Providing rules and regulations for manufacturers is the best option: telling a manufacturer that if they live up to a standard they are allowed to be sold"* (P3). *"If that becomes the standard it will take a while, but let's say a smart fridge has a lifespan of 7 years: if the last insecure smart fridge is sold today, and legislation is in place, it will take seven years before the problem is gone"(*P3). This means there is a need to define a level of security required, as well as create ways to give more transparency to users (P2). According to an ISP: *"users would pick a more secure device and would be willing to pay 20% more. This should make a manufacturer jump: relatively easy implementation, selling more, and for a higher price."* (P3).

This is already being initialized by the ETSI 303645 (ETSI, 2020), as named in chapter 4. *"Using the ETSI as a certification guideline will help. We did the same with a medical device regulation last year. Currently, no unsecured medical devices are put on the market anymore, so it works"* (P3). The ETSI is used in the Radio Equipment Directive (Directive 2014/53/EU of the European Parliament and of the Council , 2018) in very general terms.
On a national level, lacking legislation and standards should ensure no sprawl of IoT standards (Albada Jelgersma, 2020). European legislation is not yet realized, but will result in national legislation that will solve the problem for municipalities as well: *"In an ideal situation you would look at the same network data of The Hague in a few years, and see no more vulnerable devices. This depends on a European level to improve that"* (P4). *"Being able to say to vendors to look more into IoT secure devices"* (P3) would be legally possibly then. This would also ensure a certain level of security through design and make manufacturers having to provide updates for the stated lifetime (P2). Part of security-by-design is guaranteeing your device will be updated and supported for an x amount of time, *"a few years ago, a manufacturer dropped all support and updates for one of their devices, and if you want to use it to communicate to the outside world, this makes your device instantly vulnerable"* (P2). That will also be prevented by legislation.

8.2.2. Steering manufacturers

Ten options relate to steering manufacturers. Steering manufacturers relate to ensuring security by design or transparent communication to users. Directly targeting them with legislation of financial means or fines (option 23, 25, 26, 33, 34, 35) is practically impossible for any stakeholder since there are many (more minor) manufacturers abroad. It is impossible to reach all manufacturers in the world. In a legal sense, ISPs also do not want to do this (P2), and municipalities cannot do this and wait for European legislation (P4).

To make it work

"It should be done the other way around: not targeting manufacturers specifically" but setting the boundaries and levels for safe devices on the market (P2). This will influence all potential device manufacturers that want to sell. As stated in security-by-design, through European legislation used for national legislation, manufacturers can be forced to require a level of security (P4), although not implemented yet.

Steering manufacturers indirectly by only allowing "secure" devices to be used onto the ISP's networks is undesirable. ISPs do not want to exclude devices and brands from their network (option 21, 22) since that would *"get in the way of a free market"* (P2) and would *"lock brands out of the network and therefore not improve their products by design"* (P2). ISPs can provide support for certified devices (P1) or devices they provide to the customer and have thoroughly tested (P2). This is done in practice since ISPs do not feel like actively policing the network and force users to use specific devices. They only provide advice to users. *"If you want an unsecured device to tamper with, and are aware of the risks, who are we to tell you it's not allowed?"* (P2) as long as it's according to the network use agreement (P3).
Making deals with manufacturers to increase their security by giving out their devices (option 22, 24 or 75) turns the roles around. ISPs and municipalities *"should select devices that are already secure"* (P2), and that indirectly incentivizes manufacturers of insecure devices to step up their game. For the municipality, this can be applied by taking the role as device user and set a level of security required for their own (smart city) devices (P4): *"by influencing the chain they are in, and requiring a security standard (like ETSI) for the devices they use, the municipality sets the right example and is prepared for any future legislation that might come"* (P3). The municipality can not steer manufacturers for the consumer devices found in the network scan data since there is no legislation (P4).

8.2.3. Steering ISPs

As a local government, you might want ISPs only to allow devices that live up to a security standard onto the network (option 27) but to implement this locally would not work. Therefore, this option is viable as a national effort (like device legislations); however, this is not viable from the ISP's point of view (see: steering manufacturers). The same goes for pressuring ISPs to clean up vulnerable devices (option 85) or forcing ISPs to actively scan their networks and take a proactive role in solving vulnerabilities (option 75, 86). Legally, by the definition of their role as facilitator, and technically by their current means, ISPs cannot do that, *"even if we neglect the legal side, and want to do it, we do not have the technical means to check every customer pro-actively"* (P3). Remediating infected devices based on abuse notifications if legally possible, but notifying and helping customers with only vulnerable devices can already be seen as a privacy infringement (P2).

To make it work

To make ISPs act on vulnerability management instead of only on abuse management, legislation needs to be changed, technical capabilities expanded, and they need to take a different role. *"It is something that is not our business, we are not insured to do it, and it's simply legally not possible"* (P3). This would require a financial incentive, *"we (as ISP) did a small project to see if, with extra devices and services, we could offer a more pro-active role in vulnerability detection. That project ended since legally and in terms of the business case it was not doable"* (P3). This would also need customers to give permission for the ISPs to *"pro-actively look into their homes"* (P2). As an internet facilitator, that means a different role. Collaborating with other actors (ISPs, or municipalities) to actively solve vulnerabilities in IoT devices *"is a noble thought, but collaborative efforts from multiple ISPs are not viable, and this would require ISPs to start cleaning up security issues caused by IoT vendors and manufacturers which is not our role to play"* (P2).
Altogether, steering ISPs is not viable since ISPs are already acting according to the current law. Changing legislation would do more harm to the free market than good (P2), and then there would still be no relevant business case and technical means to get involved pro-actively. In terms of governance and role ISPs know exactly what they are allowed to do and do that within the boundaries of the law.

8.2.4. Steering device users

Directly steering device users as manufacturer or ISP by calling a helpdesk or provide an expert (option 53, 54) before setting up their device is not attractive for these stakeholders. Manufacturers must provide a level of support (P1) but do this through guidelines and manuals. For device brands on the other side of the world, there is a language barrier when actively needing to reach out to them (P1). ISPs have no positive business model that makes them provide this level of support and again state it's the user's responsibility (P1).

To make it work

As municipality only allowing devices that live up to a specific security standard (option 40) can be done through national (or European) legislation as discussed under security-by-design. Providing discounts for safe devices (option 41, 43), or forcing device vendors through financial compensation (option 42) can legally only be advised but not forced (P3), *"we have set up a foundation that has the goal of making buildings and houses smarter"…" We can advise people, and tell them what would be most secure. We can not force anyone to not buy an unsafe device"* (P3). Other than technical knowledge about IoT devices, this also requires defining and enforcing security standards. The municipality could acquire this knowledge through a third party. However, they do not want to take up the role of device expert to provide citizens with advice on a device or have a helpdesk: *"It would not be allowed as a government"…" other actors are doing this, and you would interfere with them"* (P4).
Collection points for old devices (option 95, 91) buying unused devices of users (option 98, 96, 92), or giving discounts when users hand in their device (option 90, 93, 97) only solves part of the problem by cleaning up, but not preventing vulnerable devices from coming to the market. *"The problem needs to be solved at the manufacturer*" (P3). Collection points would require a third party to secure the devices then or dispose of the devices safely. This again requires knowledge and costs money to set up, which is only done by the municipality once they have an incentive to do so, and the problem indicates this as a solution. However, since vulnerabilities come from manufacturers and are risks to users, they will not provide this option (P4). ISPs also have no role in this since they are only facilitators of the network (P1).

8.2.5. Informing device users

The largest category (33 options) involves informing device users, which falls in line with the roles manufacturers and ISPs take since it puts the responsibility in the hands of users. Giving information to users and have users decide what to do with this is a valid option. The way to convey this information and what this information entails differs per option and stakeholder. Some users might want insecure devices to mess with, and by providing more information, this choice will be more conscious (P3).

To make it work

Manufacturers can provide information through notifications on their website (option 67) or through the device interface (option 68). However, this would then rely on device users to actively take these notifications and solve the issues, requiring some helpdesk (option 49). It would also lower trust in manufacturers since they have to tell about how unsafe their device is. Considering this results in a negative business case, manufacturers have no incentive to pursue this more. This can only be forced through legislation, *"giving consumers different options through indicating security information on or about a device"* (P2), *"customers will pick a more secure device over a less secure device"* (P3). Tying this together with *"requiring manufactures to support and update a device and letting the customer know on the device itself"* (P2) comes down to increasing transparency by law.

Manufacturers can provide security labels (option 29) on their devices to add transparency. An internet service provider states that giving users clear information on security allows them to decide whether they take the risks for granted or pay more for security (P2). Providing information about vulnerabilities through the manufacturer's website or a helpdesk (option 30, 31) is extra support that is mostly not relevant to manufacturers but legally required during the lifetime of a product (see security-by-design). However, this assumes device users are tech-savvy, which is not always the case. *"You can provide everything, but you*

cannot stop stupidity", because *"if you need to change a password and go from Welcome123 to Welcome345, you as a user are the security risk"* (P3). That's why manufacturers do not give a warranty for their devices being safe (option 32) since they can not guarantee that and place responsibility on the device users. The same goes for the municipality, which can not set up a security label: *"This really needs to be set up on a European level*" (P4). This means that again it comes down to informing users about cybersecurity.

Organizing information campaigns about security aspects are valid options for ISPs and the municipality (option 37, 56). Currently, ISPs are already occasionally sending out general notifications to make customers aware that there could be security issues in their IoT device (P1) (option 37, 56, 69). However, there is a risk of reliance and insurance since telling people about security issues or acts to solve these issues puts the responsibility in the hands of these stakeholders. People might say: you told me I could fix vulnerability x through guideline y, which made the problem worse. *"Therefore, we do not specifically tell people we found vulnerability x on their network, and they should solve it through y"… "Only in general terms"* (P3). *"Sending an email would already work"* (P4).

As said, specific vulnerabilities found in the network scan data are not communicated to customers by the ISPs, since they only act on abuse notification (P2). General security notifications are given and require less specific technical knowledge. By being able to state users are at risk without having to specify the device or vulnerability would already *"alert users"* (P4). Sending out general security notifications can also be done by the municipality (option 64, 76) (or a third party through the municipality) but can not be targeted towards specific device users and only to every citizen in the municipality. This would be a general information campaign then, which is also already done nationally (P4).
The same goes for setting up a website or security label (option 38, 39) as a municipality to check IoT devices (which is not viable; see steering device users), or sending a letter to every citizen (option 56): not having the ability to target specific users, and the lack of specific problems means a specific campaign is difficult (P4).

The ISPs can target specific users, but only when the vulnerabilities escalate. Otherwise, there is no incentive through their business case (P1). Also, setting up a security label (option 46) or services to check how safe IoT devices are (option 47) is not profitable for ISPs. There are ISPs at the moment that advise customers on certified devices (mostly in business IoT), which is also applicable to consumer IoT (option 48), but once again only through opt-in. This means ISP can advise users by informing them (through labels (option 46) or a website (option 47)), for instance. For devices ISPs provide themselves, they have full support and guarantee safety (P2), *"if such a device becomes vulnerable, like the routers from the dataset, customers have to have pressed a button to make it publically viewable actively. Normally these settings are off by default"* (P2).

ISPs feel like they are the facilitator, which means they do not want to actively check their customers and provide services to solve vulnerabilities (unless their networks can be harmed) (P1). Therefore actively reaching out to device users (option 60, 72) after finding vulnerabilities like described in the dataset (chapter 5) is something they can do but are no motivated to do. Vulnerabilities relating to similar devices should be taken up through manufacturer support or from the store the device is bought from (P2). Similarly, creating guides on how to solve IoT issues (option 81) or setting up a helpdesk (option 52) is only done in practice for a selection of supported IoT devices (P1/P2) that ISPs facilitate themselves. There is no business case for ISPs to provide extensive support or help to customers for remediating or solving security vulnerabilities. As an internet service provider put it: *"we can provide the support that costs 20 euro for a 10 euro costing device, which is something we do not want to do"* (P1). This also relates to having experts for IoT devices (option 51, 52, 53). This requires time and money, and therefore there is a lack of financial incentive.

8.2.6. Policing IoT

The category to police IoT (9 options) involves a proactive approach from either the municipality or ISPs.

As described through the role of ISPs and in the previous categories, there is no legal ground at the moment for ISPs to actively target citizens and solve vulnerabilities before they turn into abuse notifications (P2). Setting up inspecting departments (option 36) or helpdesks (option 84) require specific knowledge for every IoT device being used, which causes a problem of insurance (P3).

Creating certificates (option 59) and forcing users to only use these secure devices (option 94, 100) as an ISP is not part of their role. As a municipality, there are no legal grounds to force people. It costs time and knowledge to set up a certificate or standard that is not the municipality's role (P4).

To make it work

Legally and ethically, these options are unfavourable. ISPs quarantining users is done (option 83) only when other users in the network or the ISP are affected by unusual network traffic (P3). Again, most ISPs have no real incentive to pro-actively solve IoT vulnerabilities that only are risks for users (at that moment). Vulnerabilities, as found in the dataset (chapter 5), do not harm ISPs and therefore they take no active role until notifications are made, and the threat harms the ISP (P2). The same goes for going door-to-door to help customers (option 62, 66). Proactively preventing vulnerabilities as ISP can technically be done by only allowing IoT through VPN tunnel (option 63) supplied by the ISP. Still, there is again no financial incentive to do this. This is now only done in business IoT applications (P1).
There is a catch, considering specific smart city IoT. If the municipality rolls out their own smart city network with their own devices and sensors, the facilitating ISP(s) can pro-actively secure this networks since the municipality owns these networks and could opt-in for this option (P2). This would make the municipality take a pioneering role as an example to secure their own networks (P3) through standards and security levels. However, since the network scan data results from public networks, these legal restrictions for the ISPs and individual opt-ins are required. The municipality can only control their own networks and devices (P4) until top down legislation arrives.

8.3. Barriers and requirements for implementation

Based on the described perspectives of each stakeholder in 8.1.1., and the explication of different governance options in 8.2, there are recurring barriers and requirements that surface through the information provided by the interviews and literature. These barriers will be addressed now, after which requirements to overcome these barriers will be described.

Recurring barriers

For manufacturers and ISPs, there seem to be incentives needed for them to take (more) action. This primarily results from (the expectation of having) no positive business case when implementing governance options or legal boundaries.

Incentive for manufacturers to invest in security
Customers keep buying unsafe devices, and manufacturers hide behind terms and conditions users need to follow. By not stopping the problem at the source, the problem will proceed. Making manufacturers more liable for the security issues in IoT. The most significant issue seems to be a lack of investment when there is no direct incentive (Levy-Bencheton, 2018). Although security-by-design seems like the best step forward to demand through legislation, it turns out that there is a delay of compliance between what should be done (regulated or agreed upon) and what is done in the industry. According to Saleem et al. (2018), this is because of a lack of economic incentives to innovate and keep security up to date since manufacturers are not the direct victim of security vulnerabilities.

Another aspect related to this is the increased production costs to keep up with security. Think about resources needed to manage software and keep it up to date for all known software vulnerabilities at that time, fix bugs, but also changing complete production lines to ensure secure devices (Saleem et al., 2018).
To encourage this, legislators should define security standards and enforce these, leading the way to more trust and resilience in IoT devices (see figure 8.1). This could also include requiring more transparent information on security aspects of devices, fines when devices do not live up to set standards (e.g. privacy issues), or a cross-sector acceptable level of security that would promote a minimum level of security (Levy-Bencheton, 2018). This would clear up the liability issue of whether it's a manufacturer or device user's fault, and inform device users.

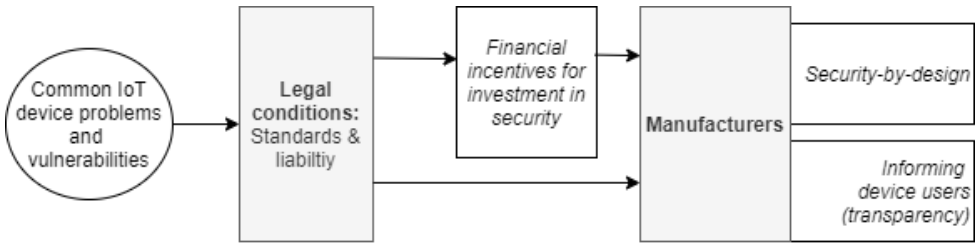

Figure 8.1 Setting standards by getting more information on IoT vulnerabilities could result in financial incentives for manufacturers, incentivizing manufacturers to implement more security-by-design.

Incentive for ISPs to provide more support
ISPs step away from providing extra support to customers by saying it is their own responsibility and also because legally it is not allowed to target specific customers. For ISPs to take an active role and prevent IoT vulnerabilities can be realized through a financial incentive. As the municipality put it: *"We might find a problem, but then we can pass it on to the ISPs and they should solve it"* (P4), which they are currently not doing or equipped for.
ISPs are commercial businesses and therefore need some financial incentive to take a more active role: either investing in the technical infrastructure combined with individual opt-ins for each customer or tailor-made solutions for each customer at home (also through opt-ins). In theory this would work, but it requires changing the ISP's role and therefore also changing legalization. This would interfere with the GDPR, free-market principle, *"and get you tangled in a web of legislations and rules"*(P4). Therefore this is practically not possible.

Recurring requirements

For manufacturers, ISPs, and the municipality, three recurring requirements are needed for stakeholders to take action.

Specification and enforcement of standards
What are the best practices and the highest level of security? This needs to be determined, periodically updated, and enforced by an authority. Suppose manufacturers are required to be transparent and add a security label. In that case, this needs to be independently checked, like an ISP that is already extensively checking the devices they give to customers (P2). This is already partly defined through general guidelines on a European level (ESTI), which a municipality could use to influence their IoT use and set an example. This would make the municipality similar to a user that decides only to use more secure devices. However, without actual enforcement through implementation, manufacturers do not have to live up to these standards. Therefore binding (inter)national standards for IoT need to be developed before manufacturers will take action.

A national or collaborative approach
The identification of vulnerabilities on a local level cannot solve issues on a national or international network. Based on local problems, a national approach needs to be informed (P4). The options a municipality has can only be targeted at all local citizens since no specific device owners can be reached. However, the municipality can only advise or inform in some way: to take specific action for consumer IoT resulting from the network data is not possible (P4).

Preventing vulnerabilities through manufacturers would result in no device users needing to be contacted first and less informing users about potential vulnerabilities. Through a national approach (resulting from European legislation), ensuring more secure devices (through legal guidelines and standards) as a means is created. However, this approach has to be targeted to include specific problems or actors that might surface locally (through implementation of a smart city, for instance). Therefore local governments like The Hague can use their network scanning initiative to inform legislation in terms of the types of vulnerabilities or devices, on a national or international level.

For public stakeholders, the first step is already there. Five major Dutch municipalities facilitate pilot projects concerning innovations and then identify barriers and solutions that the national government could facilitate (Bruines, 2018b). However, since 2017 there has been a 'roadmap soft- and hardware', focussing on IoT and development by the national government, which is not finished possibly due to a lack of clear problematization and incentives (Keijzer, 2020). In terms of collaborations to inform users, foundations like the smart home society, comprised of public and private actors with no legal ground, offer promotional campaigns aimed at more secure configurations and the use of IoT devices (P3). Without legislation in place, this is one of the best options to set up with as many stakeholders as possible (P3). "*Bringing like minded people together and progress the problem"* (P4).

Lack of problematization to take action
What are the vulnerabilities that need to be solved? What is the scale of this problem? Who should be targeted? And does the problem change over time? There is a need for a liable actor that can be targeted and more specificity in what the actual problem entails. Before any action is taken, an actor needs to take the lead to progress the problem. The municipality's primary motivation is to *"map out the problem"…* and *then "develop means and tools to solve it. Of course, you have to secure your city, but national implementation comes next"* (P4). The Hague emphasizes the use of data for decision making and insights into the city (Gemeente Den Haag, 2021) but have no precise specification on what security risks are involved and how they should be solved. A more unambiguous problem indication would incentivize other stakeholders to take action.

Relating to the dataset findings: not more data, but more conclusions

There need to be more clear quantitative insights from the data already available to address and back the problem, before governance options can even be considered *"This problem just feels like a project (at the moment)"…" There is no urgency involved, it seems. That's the most significant issue"* (P4).

However, there is no need for the involved stakeholders to have more data on IoT devices to demand resources for instance. All interviewed stakeholders mentioned no need for more specific insights, since the municipality states: *“There is no need for more data to make decisions”* (P4). And for ISPs legal boundaries in place make it impossible to perform a more active role in reaching out to users (P2), giving no need to use additional data. The idea that more specific data on vulnerable devices can facilitate more governance options for the municipality or ISPs is not accurate, and getting more specific data is not possible in terms of legislation and privacy violations. *“The next step for more specific data would be to attempt default passwords and get into a device actively: this is of course not allowed”,* the municipality says, *”We only want to stand on the curb and see if the front door is open. Everything that is not allowed, we will not do” (P4).*

That being said, a nuance has to be made: more specific additional data to identify device users is not an available option, but presenting more conclusive insights on the current available data is. Even though the data itself was not confident or fit to identify specific users (Jaquith, 2007), it still makes the problem more tangible and therefore can increase urgency. In terms of data management a third party (e.g. a network scanning company like Cybersprint) (non-ISP or public) can fill the need for more conclusive quantitative data insights on the data that is currently available and gathered.
Not concluding *there are indeed vulnerabilities,* but saying *there seems to be an x number of similar devices, and concluding an x number of vulnerabilities occurring an x number of times* will give a higher felt urgency when presented to other stakeholders by the municipality.

This does not necessarily mean to fingerprint more devices or scan more networks. As the data found that there is no 100% certainty about the devices and vulnerabilities found, but there is still an indication of vulnerabilities present that result from the current data. The lack of ‘leading actor’ as specified by the municipality, but also no need for more or different data also stated by the municipality, indicates that presenting quantitative conclusions from current data should be used as incentive for municipality to take this leading role themself, and use their findings to make other stakeholders act.

8.4. Conclusion

The identified stakeholders all realize the problem that vulnerable IoT devices can pose for device users. There are legal boundaries role restrictions for the municipality and ISP in terms of options, and a lack of problematization keeps the identified stakeholders from acting on the problem.

The current perspectives

Manufacturers have no incentive to solve security issues pro-actively and keeps pointing at users being responsible. They need legislation to start moving towards more secure devices. The municipality recognizes that security issues involve IoT but feels like they have no active role in this. They only want to look into the problem and have other stakeholders fix it. As a municipality they can only lead by example and wait for legislation to be in place. When signalling the problem of vulnerable IoT device from having their public networks scanned, they pass it on to ISPs to fix it.
However, ISPs have a vital role in the literature, and they seem to recognize the problem. Still, in reality, they see it is not their role to fix it or provide support: pointing at users responsible for the way they handle IoT and manufacturers for implementing security-by-design and setting security standards. Framing ISPs as the essential stakeholder to contact device users neglects a layer of legal possibilities, privacy issues, incentives, and the free market behind it (P2). Therefore it is concluded that ISPs are doing everything they can according to the legal boundaries at the moment, and changing this would do more harm than good.

Most viable option

The most viable options at the moment are informing device users (through the different ways addressed). Enforcing more security-by-design seems the best option in terms of tackling the problems at the source (chapter 7), and it is favoured by ISPs and the municipality. However this requires international legislation to become feasible. Therefore, by giving enough transparency about a device's security and making users aware of security aspects, it is possible to ensure less vulnerabilities surface through a lack of security-by-design. Setting up information campaigns as a municipality or ISP and collaborating with other actors is most viable also since network scan data can only go so far in providing specific IP information and the role of ISPs (as expected in chapter 7) proved to be limited. While waiting for legislation on devices informing is the best option. To incentivize collaborating, quantitative findings on the problem can create more urgency at the defined stakeholders (as discussed previously).

Where can stakeholders work together?

The discussed information from the interviews, literature, and described analysis can be found in table 8.1. The discussed options are executable from a single stakeholder perspective, but the efficiency and validity of options rely on other stakeholder involvement (table 8.1).
The municipality wants to gain more insights into the IoT problem but perceives a lack of a leading actor or incentive to proceed. As the municipality, they cannot provide the solutions but can fulfil their condition and become the leading actor that pushes the problem forward. They can do this by gaining more quantitative insights to be able to indicate: this is the problem we want to solve by information campaigns. This creates an incentive to progress the problem.

The next step is to get the other stakeholders involved by stating the situation through the current data insights. Creating public-private partnerships to create an information campaign specifically targeted to IoT vulnerabilities from the dataset. The municipality can indicate the problem to ISPs through the third party data, and (within the law) they can freely advise and notify users in general about IoT safety. Manufacturers will only invest in more security through legislation, but getting them involved to inform device users better about using a device has a low cost. It would be attractive since it makes the manufacturer less liable for vulnerabilities. This overlaps with providing security labels, which has to wait for legislation to be pursued by manufacturers. Until legislation arrives, generally informing devices users by all stakeholder is the best next step.

What is needed for this?

As shown in figure 8.2, the municipality has a general attractiveness to act, indicated by the role they are willing to take. They cannot act at the moment since they have no specific quantitative conclusions to indicate the problem and rely on other stakeholders to solve the problem they identify. So for the other stakeholders to start moving, the municipality has to take this step. When it comes to ISPs, they know their role and legal limitations and do not feel attracted to act. Legally their capacities are also more limited than expected from the literature. When it comes to manufacturers, they have the capacity to act and play an active role in solving issues. However, due to the lack of incentives, their attractiveness to act seems low. Device users are plotted with a low capacity to act since vulnerabilities that result from the device itself, or a lack of information on the device should be solved through other stakeholders.

Table 8.1 An overview of the governance options, favoured stakeholders, and potential requirements.

Type of option	**Favoured by stakeholder:**		**Verdict/condition needed**
Security-by-design	**Manufacturer:** No **Internet Service Providers**: Yes **Municipality**: Yes	**Collaboration possible?** Yes, ISPs and municipality	*Incentive for manufacturers to invest in more secure devices:* - Financial incentive - Legal incentive - Pressure through users (consumers, businesses, ISPs etc.) to only start using secure IoT devices. **<u>In need of:</u>** European legislation or national legislation.
Steering manufacturers	**Manufacturer**: No **Internet Service Providers**: No **Municipality**: Yes	**Collaboration possible?** No, only the municipality	*Incentive to steer manufacturers into security-by-design or more transparency:* - Financial incentive→ Users pay more for security or fine manufacturers that lack security - Development of technology standards - Legal incentive → Enforcing security standard - Pressure through users (consumers, businesses, ISPs etc.) to only start using secure IoT devices. **<u>In need of:</u>** European legislation or national legislation.
Steering device users	**Manufacturer:** No **Internet Service Providers**: No **Municipality**: Yes	**Collaboration possible?** No, only the municipality	- Development of security standards → Adding transparency through security label - Legal incentive → Enforcing security standard **<u>In need of:</u>** European legislation or national legislation.
Informing device users	**Manufacturer**: Yes *(by providing more information through security labels),* No *(by providing notificaitons and monitoring through device)* **Internet Service Providers**: Yes **Municipality**: Yes	**Collaboration possible?** Yes, ISps and municipality	*Most viable options, requires:* - Incentives for manufactures - Incentives for ISPs - Development of security standards - More urgency to solve the problems involved with IoT - A collaborative approach **<u>In need of:</u>** - More insights to indicate urgency and progress problem→ mobilising stakeholders to get involved. - European legislation or national legislation.
Steering ISPs	**Manufacturer**: No **Internet Service Providers**: No **Municipality**: Yes	**Collaboration possible?** No, only the municipality	*Incentive for ISPs to provide more support:* - Financial incentive → No business case - Customer opt-ins → Technically not possible - Legal changes → Will harm the free market.
Policing IoT	**Manufacturer**: No **Internet Service Providers**: No **Municipality**: No	**Collaboration possible?** No	- Legally not possible by ISPs. - Requires public networks to be privately monitored: dictatorship, and infringement of legislation. <u>Unfavourable.</u>

Based on the overview of findings in table 8.1 it shows that steering ISPs is no valid option in terms of the perspective ISPs have on this and the boundaries in place. Having no business case, being technically not feasible, and having to change legal conditions make this option less favorable. Other than that there are no means for municipality to actually pursue this option. The same holds for the policing IoT option since it is not preferred by all three stakeholders, legally not possible to implement, and would again infringe with legislation in place.

Figure 8.2 highlights the lack of a single stakeholder with the capacity to implement and be attracted to implement governance options. By giving the municipality presentable insights into the IoT problem through a third party like Cybersprint (as a means to showcase the problem), the municipality acquires the capability to progress the problem. Having this act as an incentive to set up collaborations, and the position of stakeholders should shift into the upper right corner with all stakeholders becoming attracted to fix the presented problem (with ISPs able to provide in information campaigns, and devices users more knowledgeable and therefore more able). Based on this collaboration, informing device users is the next step forward while waiting for European (or national) legislation to solve the manufacturers' side of the problem. This will be further addressed in the next chapter.

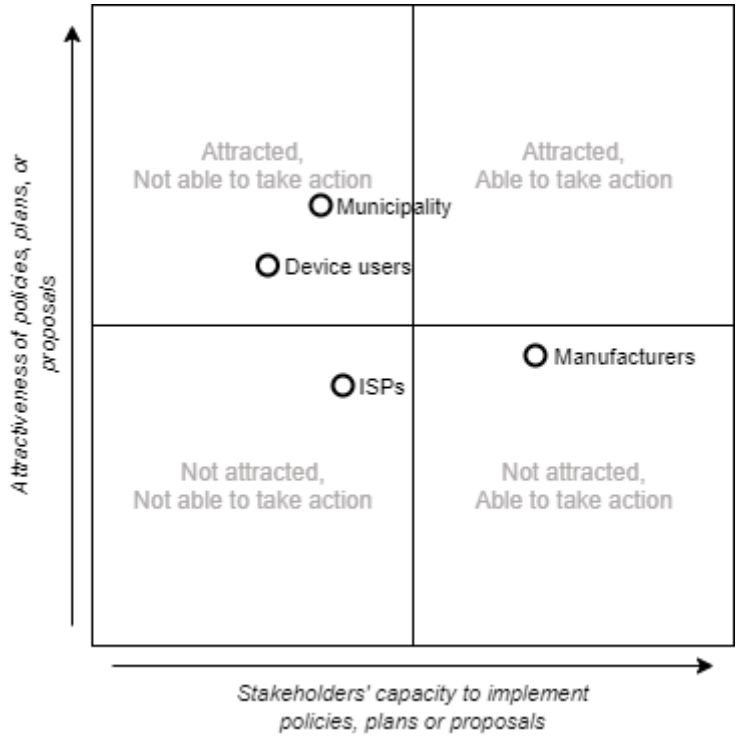

Figure 8.2 the attractiveness to implement policies or plans versus the capacity of the stakeholder to implement these policies at the moment. (Bryson, 2007)

9 Synthesis and framework

Previous findings will be combined in a conceptual framework to structurally gain insights into the options as well as their conditions. This will answer research question 7, being: How can these governance options be used to reduce the presence of vulnerable IoT devices?

9.1. Framework

The reason to use a framework is to synthesize the findings from previous research questions. This framework is used as a structure with existing definitions and concepts that structure the findings within the area of research (Abend, 2008).

9.1.1. Conceptual framework

The concepts defined in the literature review of chapter 4 will be used to structure the findings of chapter five till eight into an empirical framework. The proposed conceptual framework will be filled in using the following information:

- ***Stakeholders****:* derived from the data exploration in chapter 5 and 6 (sub-question 3 and 4).
- ***Governance categories****:* derived from the selection of options and validation in chapter 7 & 8 (sub-question 5 & 6).
- ***Governance structures****:* taken from the literature review in chapter 4 (sub-question 2).
- ***Barriers for implementation****:* taken from the validation in chapter 7 (sub-question 6).
- **Governance principles**: taken from the literature review in chapter 4 (sub-question 2).
- ***Requirements/criteria for implementation****:* taken from the validation in chapter 7 (sub-question 6).

Based on these concepts, the proposed conceptual framework is shown in figure 9.1.

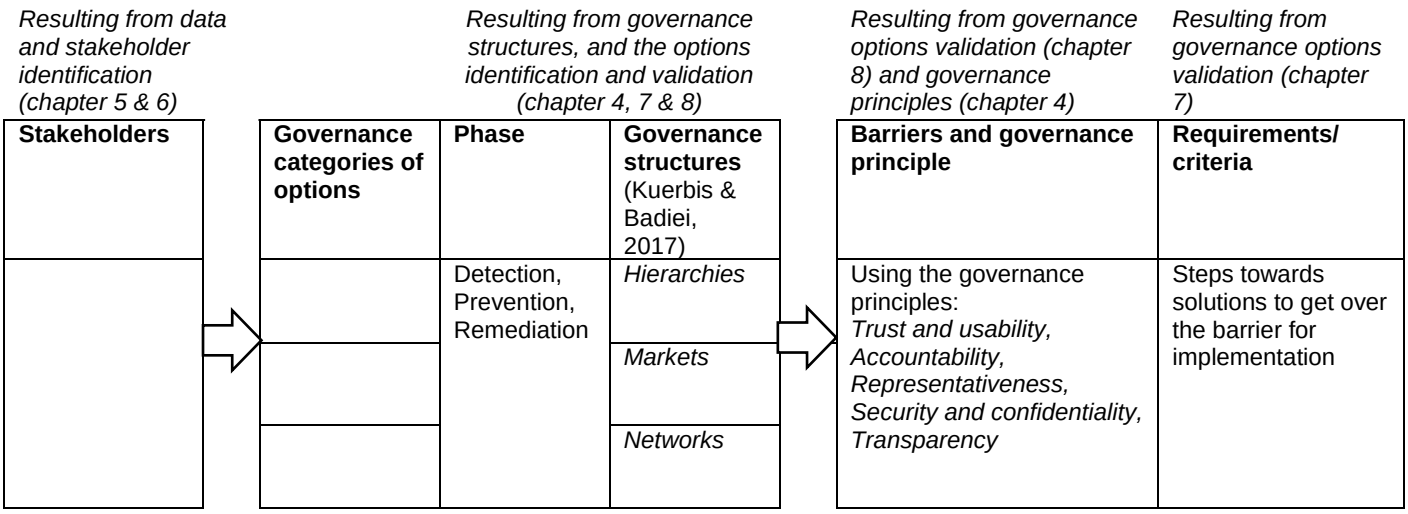

Figure 9.1 The conceptual framework used to structure the findings of this research.

9.1.2. Empirical framework

By filling in the conceptual framework with the findings of previous sub-questions, the empirical framework of figure 9.2 is created. Through this framework, validated options for each stakeholder are structured.

Stakeholder	Governance categories	Phase	Governance structure	Barriers	Requirement/criteria
Municipality	1. Steering manufacturers	*Prevention*	*Hierarchy*	- Insufficient information to progress problem: no incentive to act **(representativeness)**. - Lack of technical knowledge **(trust and usability)** - Lack of stakeholder liability (**accountability and representativeness**) - Legally not possible to look at ISP data (**transparency, security and confidentiality**)	- Investments to incentivize manufacturers (discounts at vendors, fines through standards and legislation) - Define security standards for devices (national/international regulation) - Collaborative effort (national or municipal) with third party to acquire more insights - Collaborative effort with multiple actors to inform and advice device users (through public-private partnerships and foundation).
	2. Steering ISPs	*Prevention*	*Hierarchy*		
	3. Steering ISPs	*Remediation*	*Hierarchy*		
	3. Steering device users	*Prevention*	*Hierarchy*		
	4. Informing device users	*Prevention*	*Markets*		
	5. Informing device users	*Detection*	*Markets*		
	6. Policing IoT	*Prevention*	*Hierarchy*		
Device manufacturers	1. Security-by-design	*Prevention*	*Markets*	- No incentive to improve security: people still buy products **(trust and usability)** - No incentive to invest in security efforts **(accountability)**. - Technical limitations (**trust** & **usability**)	- Improve cybersecurity attitude of device users - Economic incentive for security investments - Legal incentive for security investments
	2. Informing device users	*Prevention*	*Markets*		
	3. Steering device users	*Prevention*	*Hierarchy*		
	4. Informing device users	*Remediation*	*Markets*		
Internet Service Providers	1. Informing device users	*Prevention*	*Markets*	- Role as network facilitator and not control the network (**trust & usability**) - Lack of incentive to actively support and guide people setting up/using IoT (**accountability & transparency**) - Legal restrictions to pro-actively look for vulnerabilities (**accountability**)	- Legally have ISPs be able to act preventatively on vulnerabilities, before abuse notifications → Provide opt-ins for every customer (technically not feasible). - Financial incentive for actively supporting and guiding people (no business case).
	2. Informing device users	*Detection*	*Markets*		
	3. Informing device users	*Remediation*	*Markets*		
	4. Steering device users	*Prevention*	*Hierarchy*		
	5. Informing device users	*Remediation*	*Markets*		
	5. Steering manufacturers	*Prevention*	*Hierarchy*		
	6. Steering manufacturers	*Detection*	*Markets*		
	7. Policing IoT	*Prevention*	*Hierarchy*		
	8. Policing IoT	*Detection*	*Hierarchy*		
	9. Policing IoT	*Remediation*	*Hierarchy*		

Figure 9.2. The filled in empirical framework.

9.2. Analysis based on the framework

Individual actions are not governance since governance relies on the other stakeholders as well. For instance, public stakeholders create legislation and rely on other stakeholders to actually follow this regulation. Relating back to multistakeholderism (chapter 4), from the empirical framework, a lack of network governance options becomes evident. The defined governance options mainly involve single stakeholders that implement options dictating to others what to do (hierarchical) or have stakeholders give out information in order to have others react to this (markets). As shown in the previous chapter, there is no single stakeholder that by itself can implement governance to solve IoT vulnerabilities.

The policing of IoT options showed to be no valid options in chapter 8, similar to the steering of ISPs since the role of ISPs is shown to be limited by the barriers and requirements needed to overcome these barriers. Looking at the boundaries through a security economics lens shows that underlying barriers for implementation result from a lack of incentive by the private stakeholders (ISPs and manufacturers) that feel no accountability or need to provide more transparency about IoT issues, and a lack of problematization by the public actor(s) (the municipality of The Hague) that can only go so far in terms of legal and technical means. Now the steps needed to implement will indicate how the options can be used, with the municipality as the leading stakeholder (as described in their role, chapter 8).

1. Focus on prevention and data conclusions (bottom-up)

Prevention of vulnerabilities through governance options seems like the best options. This can be done through informing or steering device users into more secure devices or security practices or making sure devices are more secure by design.

However, these are hierarchical measures that force other stakeholders. To have a legal ground to do this, a liable actor needs to be found and held accountable: with a lack of problematization, the steering options of the municipality cannot be targeted towards a specific stakeholder. This halts the problem and does not provide representable governance. To gain more problem insights locally is a difficult task (considering IP locations; see chapter 5), and considering the legal boundaries as well as data bias that is involved with gathering network scan data.

Therefore scoping the collection of data to a geographical scope will make it able to, with the same information but a more extensive dataset, determine a liable actor. Considering the legal aspect of ISPs not being allowed to scan their networks and provide this data, there should be a collaboration with a third party that provides quantitative insights from the data. As the current data should be able to give black-and-white conclusions on the number of devices, types of vulnerabilities, and increasing or decreasing magnitude of the problem (as characterized in chapter 8). Only no specific devices users are identifiable. This information can be used by the municipality to mobilize stakeholders into setting up a public-private partnership. This can be seen as forming a narrative (Borrás & Edler, 2020), as described in chapter 4. Also, this can be used as a backbone to inform national legislation and define what standards should be in place since it gives the ability to target the governance options towards a liable actor resulting from the data: targeting accountability.

2. Wait for (inter)national legislation (top-down)

By waiting for legislation, steering manufacturers or device users through rules and legislation becomes possible. This is done (more) forcefully, and therefore a hierarchical option. These options can only be implemented with relevant legislation in place since there is no ground for any governmental actor to do this at the moment.

Once European legislation is in place, there is less need for detection and remediation governance options since all stakeholders involved believe the device vulnerabilities can mostly be fixed through manufacturers. Legislation forces investments in security for new devices. Therefore it will take a number of years before vulnerable devices are replaced with more secure new ones. While there is no legislation in place, informing device users remains the best option for the stakeholders involved. The best way to do this is through collaborating.

3. Increase security practices by informing device users

Informing users is a market-based option since no transaction is forced, and by providing information or advice, it is up to users what they do. This requires users to be able to make a decision on information provided and therefore relying on the knowledge of a user. As a single ISP or municipality, you can set up (relatively) small information campaigns through the options provided (chapter 7), but with the municipality as the lead actor dependent on other stakeholders, there is a need for collaborations.

4. Collaborating within the chain

At the moment, with a lack of actionable legislation as well as means to specify the problem, the most viable option is to inform (potential) device users about device security (chapter 8). Acting as an example, municipalities can already take a leading role by setting the condition only to use IoT that lives up to security guidelines for their own IoT and IT. This would show leading by example. As the different stakeholders showed an interest in better-informing device users, setting up a public-private collaboration would transform this option from market-based governance to network-based governance aimed towards the user.

Requirements for this would be identification of the problem through quantitative conclusions from the available network scan data (as described at point 1). In this perspective, to progress the problem, the municipality can not only involve ISPs or manufacturers by presenting them with a number from the data, but also possibly vendors, installers, postal companies, or any other actor that in some way is involved with IoT could result in advice and help device users (as described in chapter 8). There are no legal grounds to force users, but advising and helping through a collaborative effort can go a long way.

The (same) new role of ISPs

This means that ISPs provide in generally informing device users and still not actively reaching them about vulnerabilities since legislation will not allow ISPs to look for these proactively. Doing this would hinder the trust and usability of the network. However, hypothetically through individual opt-ins, ISPs are allowed to do this. They only actively step in when their network is misused, and through this, hide behind accountability. At the moment, there is no ground to change their role and legislation, and there is no economic incentive to provide the active network scan option to every customer explicitly. Getting more customers to opt-in for such network scanning would increase transparency by telling them the potential vulnerabilities related to their device, but the technical infrastructure to do this is not present.

9.3. Conclusion

The power to change the current situation is not in the hands of a single stakeholder. It relies on developing legislation from national and international bodies that create accountability and liability. Only through the setting of standards and expecting a certain level of security will vulnerabilities decrease.

At the same time, while waiting for these legal conditions, a better specification of the problem can increase transparency and trust between stakeholders. The outcome again showed that in terms of possible steps for stakeholders to take, the municipality would have to be leading/initiating. By taking the municipality as a lead actor and taking quantitative conclusions from the available data, the municipality can indicate the problem to get stakeholders involved, which helps to create urgency in solving it. Current data conclusions only indicate a problem but not give black-and-while quantitative conclusions. Using a third party to gain more confidence in determining devices, more extensive scope of the data, and more specific conclusions will result in getting ISPs and possibly other actors related to IoT (vendor, municipalities, IT companies etc.) on board to solve the issue.
The best option (before top-down legislation) is to increase cybersecurity knowledge at users collectively. Turning market-based governance by providing extra information into network-based governance through collaboration between these stakeholders (like the smart home collective or different consortia at the moment). This option aimed at users does not rely on other governance options to be taken first (like waiting for legislation) and is able to solve a big part of individual vulnerabilities on the user's side. On the manufacturer's side, the boundary remains legislation against manufacturers.

10 Conclusion

After answering the sub research-questions through this research, the acquired information will be used to provide an answer to the main research question: How can the municipality of The Hague use governance instruments to decrease cyber vulnerabilities in IoT devices? After answering this research question the overall relevance to the CoSEM programme will be discussed.

10.1. Overall conclusion

To establish a smart city, consumer and business IoT will be combined. IoT devices bring risks for individual users, with vulnerabilities that result from countless services and heterogeneous devices having to connect in similar networks and communicate with a lack of standards. As found in chapter 5, scanning the networks of The Hague by Cybersprint indicated device vulnerabilities resulting from consumer devices that are risks for individual device users. However, this data does not clarify this problem: the data is not specific enough to identify users, only contains consumer devices, and is not enough for the municipality to develop specific legislation on at the moment.

The leading role that was expected of the municipality of The Hague in solving IoT issues considering smart city development is partly true. Looking at the available governance options and validations from chapter 8 and the synthesis in chapter 9, the municipality seems to have a facilitating role. At the moment, there is a lack of incentives to implement governance to make IoT devices more secure since legal or financial governance options are not (yet) backed by national legislation or a real problematization. Through the initiative to network scan the area of The Hague, there is data available. Considering the role stakeholders (other than the municipality) can take, there is no lack of data needed to mobilize these stakeholders. There is a need for quantitative insights from current data, which a company like Cybersprint could provide, that makes the identified problem tangible: "*there are an x amount of devices from these brands, with these specific vulnerabilities which means they can be solved by manufacturers doing x or users doing y*"—taking the uncertainties of identifying devices or location as found in chapter 5 for granted. Being able to present quantitative findings that indicate a problem is a powerful means for the municipality to get more stakeholders involved and become the leading actor.

However, decreasing uncertainty could be done by increasing the scope of the data to a national approach (in terms of the networks scanned). By identifying the problem of IoT vulnerabilities on a city level, indicating this problem to the Dutch association for municipalities (Vereniging Nederlandse Gemeenten or VNG) to scale up and put it on the national agenda could be the next step. This results in conclusions from data not only being able to inform other stakeholders and progress the problem for the municipality but also inform national legislation on this problem. This falls in line with the ambitions of the municipality as found in chapter 8: not only looking citywide but providing the first steps to give more insights into IoT vulnerabilities nationally. Other than this problematization, there are two simultaneous approaches for the municipality to take at the moment:

Targeting manufacturers

At the moment, European legislation is being developed, which will result in national legislation. Only after such 'top-down' legislation, manufacturers or users can be steered through standardization and required guidelines as found in chapter 9. Based on the network data, the municipality indicated they want to gather IP addresses of vulnerable devices and have ISPs decide what to do with them (chapter 8). ISPs have a vital role in detection and remediation when it comes to disturbances in their network or harming other internet users. However, they do not have a role in vulnerability detection that involve single users and does not (yet) harm their network. Also, suppose governance instruments aimed at manufacturers are successfully implemented, leading to more security-by-design. In that case, there is less need for an ISP even to take on

this role and only remain the network facilitator. So ISPs are more in need of governance options targeted at manufacturers.

Collaborating in informing

To actively lead the problem into solving, the municipality of The Hague will be required to showcase the problem to other stakeholders through the available data. Being able to show the problem quantitatively will get other stakeholders alerted and involved. This creates the urgency and means to set up a public-private partnership, intending to actively campaign (locally or nationally) for safer cyber security practices or device usage. Since no specific targeting of device users is allowed or possible by the municipality (or any stakeholder), joining forces with other IoT related actors will gain the most traction. For instance, device vendors, ISPs, other municipalities (also resulting from the dataset through GeoIP), or universities, with the shared goal of increasing knowledge by informing users and decreasing vulnerabilities.

Different actors also have different audiences (e.g. other municipalities have a different group of citizens, ISPs have their customers, and universities give an academic audience). All these different actors can share their perspectives on the problem identified by the municipality. By partnering up with such actors, the problem will gain more insights, but collaborative information campaigns can reach more (potential) device users through these actors. This would increase the chance of successfully solving IoT vulnerabilities. This can also be done as a national approach while being led by the municipality as initiator.

To conclude, with a complex web of rules and legislation regarding scanning networks, the municipality can manoeuvre through this and pro-actively start solving IoT vulnerabilities on the user level. By first gaining conclusions on the problem through the network scan data provided by a third party (resulting from what is possible in terms of networks scanning), then using an unambiguous problem identification to inform other stakeholders about this problem, and put it on the agenda of the VNG or scale it up nationally. Also setting up urgency and collaborations to start informing as many (potential) device users as possible while also gaining more perspectives on the problem identified through the perspectives of these different actors. These are the actions the municipality can take to solve the issue from a user's perspective while waiting for top-down international legislation to be in place, which will solve the standardisation issues from the manufacturer's perspective through security-by-design.

10.2. Societal and managerial relevance

The societal relevance as identified in the first chapter is reflected in the conclusion. This research provides more understanding to a problem identified by literature and the interviewed stakeholders. By researching the network scan data and the different governance options described next steps towards solving IoT vulnerabilities can be found. As stated in the conclusion, this will not only benefit the municipality of The Hague but can also benefit a national solution. Therefore the societal relevance can be increased from local to national, using this research as a starting point. The identified problem of heterogeneous devices in different networks with vulnerabilities for the users are not specifically only found in The Hague. This research provides an empirical context to an otherwise general problem (implementing governance of IoT devices) which could raise awareness of the problem. By identifying this problem in the context of The Hague it becomes more tangible. Through doing so the stakeholders and means become more relevant. The next step could be to expand this research (see 11.4: Recommendation for future research).

In terms of managerial implications this research gives a recommendation and provides a conclusion on the next step(s) to take for the involved stakeholders. The outcome of this research can be used to develop a better problematization by the municipality, in order to get other stakeholders involved. In this way this research shows why this problem is challenging to solve and if a stakeholder were to take the lead (the municipality) what they could do. These insights can be used as starting point, although limitations are present (see 11.3: Limitations) and future research will add to the current research findings.

10.3. Relevance to the CoSEM programme

The main goal of a CoSEM engineer (and research) is designing some intervention or solution to a contemporary socio-technical problem to improve the system or solve a problem (Ruijgh et al., 2019). The internet of things can be seen as a socio-technical system, with people, social interaction, and required resources on one side, and enabling technology that makes this possible on the other side. The problem identified in this socio-technical system can be generalised to managing stakeholders and technology through governance to prevent vulnerabilities. The complex aspect of the system is characterised by smaller parts that behave by themselves and create emergent behaviour (Ruijgh et al., 2019). For IoT devices of The Hague there is no single 'IoT system'. Instead, many sub-systems together form the system that needs to be managed through IoT governance. Different users, devices, networks, protocols and standards, etc., that all behave in their own way. The complexity is also formed by the presence of a multitude of stakeholders. Typical for a CoSEM research topic is the combination of public and private domains, which also is the case for this research. This combination of people and technology create uncertainties as found in this research, and indicate no single solution. By systematically researching this topic, real-life interventions are proposed in order to improve the scoped socio-technical system and decrease complexities. Contributing to guidance and insights (through this research) on defining governance related to IoT, not only for the municipality of The Hague but also for other stakeholders involved.

11 Discussion

This research is only a step towards understanding what stakeholders can potentially do in terms of IoT governance. The scientific contributions will be discussed, and the limitations highlighted. After this, suggestions for future research will be made.

11.1. Answering the research questions

The literature reviews in chapters 3 and 4 to answer research questions 1 and 2 provide background knowledge on IoT and governance for the rest of this research. In terms of answering the sub-questions, this was done successfully but could be made more comprehensive regarding IoT, security, and governance. Involving more literature, from different sources. Adding more richness to the defined concepts and to back up later findings more. However, that being said it is impossible to read all literature.

For the data analysis done in chapter 5, to answer research question 3, further analysis could provide more information on the dataset (will be addressed in 11.3: Limitations). In terms of defining what stakeholders to involve a further distinction can always be made, by not saying ISPs as a single stakeholder in general, but splitting them up into consumer and business-related ISPs for instance.

The boundary of research in chapter 7, when looking for governance options, is that there are no finite amount of options. Therefore options can always be added to the list, making it difficult to assess when the right amount of options is present. Answering the question of what options are available is done by providing the collection of options, but it makes it difficult to assess when enough options are defined.

When validating these options in chapter 8 the perspective of ISP representatives and a government representative is used. These are only four interviews, meaning that the interviewees' judgment calls can always be strengthened by getting more perspectives involved. There were no manufacturers interviewed, which would make the research findings in this chapter stronger. This means conducting more interviews with other stakeholders.

To conclude, the research questions are successfully answered and contribute to the scientific literature (see 11.2: Scientific contributions) but can always be improved by expanding the research (see 11.3: Limitations). These points will be addressed now.

11.2. Scientific contributions

This research did not solve vulnerabilities in IoT devices, but it added detail to the current body of knowledge and further strengthened assumptions from literature. An empirical context was added by using the dataset of The Hague, which contextualized existing assumptions or findings in the literature. Contributions of this research concern the following points:

This research gave examples of governance options to find out why options work or not work in a real-life context and looked at the possible next steps. This approach adds detail to the general claims in literature that briefly state the need for IoT governance (for example: Hossain et al. (2015) and Zheng et al. (2018)). Contributing to the notion that governance of IoT is a challenge (according to literature like Granjal et al. (2015) and Hossain et al. (2015)), it was found that in a real life context there is a recognition of the problem but no incentive to start solving the problem, which adds detail to the general claim on ‘governance is a challenge’ from literature.

This research contributes to the literature on the role of ISPs in solving vulnerabilities by finding that there are legal restrictions and incentive problems. For example, literature like Cetin, Ganan, Altena, Tajalizadehkhoob,

et al. (2019) and Van Eeten et al. (2010) look into the role of ISPs to act once their network is at risk. Indicating the role of ISPs is important and can solve issues by contacting (or quarantining) the users. There is also literature saying there is a lack of communication channels to provide actionable information to users (Cetin, Ganan, Altena, Kasama, et al., 2019). To add an extra layer of understanding to this literature, when it comes to vulnerabilities that are no risk to the ISP's network directly this research found that it's not favored or even legally possible for ISPs to act. This also adds to the finding of Cetin, Ganan, Altena, Tajalizadehkhoob, et al. (2019) that say quarantining through ISPs is effective but not widely deployed because of lacking user information.

On a similar note this research highlighted that user awareness and improving security practices is still found to currently be the best step forward to tackle IoT vulnerabilities, while no standardization or legislation is realised. This is discussed in literature (for example: Alladi et al. (2020), Emami-Naeini et al. (2019), Hsu & Lin (2016), and Marky et al. (2020)), and even though initially this research stated when defining the knowledge gap that this was undesirable, it is concluded with stating informing users is one of the most a viable governance options at the moment. Adding to the literature about strengthening a user's security practices.

Also, through analysis of the different governance options and the roles of different stakeholder the need for legislation and enforcement in the form of standardization became clear, as generally described in literature already (for example: Alaba et al. (2017), Miorandi et al. (2012)). As also stated in literature, this research contributed with the finding that a lack of standardization is seen as the source of vulnerabilities. In terms of added detail this research added the perspectives of ISPs and a municipality, to conclude that the expectation is that standardization from the manufacturer's side can prevent IoT vulnerabilities. This is similar to developed guidelines (as found in chapter 4; ETSI (2020)) and conclusions from literature stating that increased security-by-design would help prevent vulnerable devices (for example: DCMS (2018) and Melzer et al. (2020)).

The use of network scan data and interviews adds context to general claims in literature about current situation of solving IoT vulnerabilities. Using this context gives possibilities, but by using this data and research methods there are also certain limitations this research cannot solve. These will be addressed in the next paragraph.

11.3. Limitations

Data uncertainties

The most significant uncertainty is the total scope of the problem. The data selection bias addressed in chapter 5 causes the challenge of being able to say whether data on IoT devices is complete. You can not conclude on devices that are not found in the dataset or that are not fingerprinted (yet), while these might be vulnerable as well. Without knowing the total number of devices in an area, it can not be concluded what the scope of the problem is. This makes it a challenge to determine if the dataset used is representative or are there still many devices vulnerable that simply are not included in the data (yet). These uncertainties originate from whether a device is safe and therefore not viewable. If device is still unsafe but not found or fingerprinted in the data it will not be classified as vulnerable. Not finding a device does not mean a device is safe.

Concluding from the network data in chapter 5

There are always uncertainties when looking at the scan data since fingerprinting devices is not waterproof. Knowing the type of device, brand, or software version can never entirely be done with 100% certainty. Therefore getting more quantitative insights from the data can only be done when the data uncertainties (described above) are accepted. In other words, even by increasing the data scope, uncertainties have to be accepted to conclude from the dataset within data scanning. Finding a percentage, number, or other measures to indicate when IoT becomes a real problem and when it is not a problem is unclear and should be looked into.

Legal aspects of network scanning

To execute network scanning, there are lots of legislations to keep in mind. The border between a 'noble act' to gain insights into the problem and 'steps towards hacking' is very slim and can be considered a slippery slope. ISPs are not actively scanning their network since, in case of a dispute, a judge might rule that the ISP was committing an act of hacking. Third parties that are not ISP have less legislation since they do not facilitate the network. However, the boundaries between legal and illegal are not black and white. Port scanning devices is not illegal, but it is dependent on intentions. However, trying to find the web interface belonging to the device would require the permission of the device owner to access it. A loophole can be used by using data from another third party (e.g. Shodan, based in another country). This means another third party collects the data, and by using their data, it's not illegal while collecting data yourself can be. This indicates the difficulty in legal aspects of collecting data through network scanning, which is a challenge.

Identified stakeholders

From the dataset, the identified stakeholders are simplified for the sake of research. There could potentially be many more actors involved that go unnoticed from the data. The problem of IoT governance can be viewed nationally or internationally. The internet is global, and device manufacturers are primarily international. By looking at it internationally, the scale of the problem is too big to grasp considering the number of stakeholders involved, but that would be the real-life scenario.
For example IT companies that manage or install devices and networks. These could be categorized as 'users' or 'device owners' while actually being an extra stakeholder between the real user and the device manufacturer or vendor. That being said, perspectives and policies per stakeholder can also differ, so referring to 'ISPs' or 'manufacturers' as a single group is also a generalization of their perspective.

Stakeholder perspectives

The interviewed ISPs and municipality all showed their perspective on the situation and identified problem. They also gave their views on the possible governance options. Although they validate it through their expert opinion, it is only their judgement call and impossible to tell if that it is the only valid opinion. The information gathered came from three ISPs, which could indicate certain governance options are probably told to be less viable or reasonable coming from their perspective. The government perspective came from one municipality representative, which means their expert opinion can not be checked with interviews from other government officials telling the same thing or something contradicting. This indicates a bias from the selected participants by the gathering of data through interviews.

There was no manufacturer interviewed, which means a bias in the gathered information from the interviews. Manufacturers could provide their view on the information, perspective, and governance options. Giving reasons why security-by-design might not be a valid option or how it might work differently. The reason why manufacturers did not respond to the interview request is unclear, they could be not interested or have no incentive to cooperate with research. This also means that there could be other valuable stakeholders, experts, ISPs etc., that could give a different perspective. Adding more perspectives (meaning: to interview more knowledgeable people about this topic) would increase the validations done in chapter 8.

Innovations within IoT

By looking at data as a snapshot to identify vulnerabilities within IoT and finding governance to solve these vulnerabilities, you do not take innovations into account. Looking at the lifetime of devices and manufacturers 'reusing' old devices (as remotes, for instance) are individual IoT innovations that can be perfectly secure but not considered by designing governance. In this research older devices are either unsupported, in need of disposal, or require an upgrade. Innovative uses for older devices or backported software targeted as vulnerability are all not considered by looking at only a dataset of network scan data. Also, implementing security-by-design will not fix vulnerabilities overnight, just like informing device users. Therefore, after implementation of governance, many months or even years are needed to see the effects. Thus, giving time to innovations, which could render current governance useless or in need of updating.

Domino effect of governance options

The governance options discussed, of course, rely on certain conditions. By going through the different stages and types of governance options, prevention should be more important than detection or remediation. Also, through stakeholder interviews stopping vulnerabilities before they surfaced seemed like the best option.
This means that the most significant stalling factor at the moment, actionable legislation from the national government, could potentially create a domino effect that would make the subsequent detection and remediation options unnecessary. Furthermore, if there are defined security standards for a European market, manufacturers would have to implement more security into their devices, requiring users to be less tech-savvy to configure and use their device securely, resulting in less need to steer or inform users.

11.4. Recommendations for future research

Based on the conclusion and research limitations there are certain directions future research can take and research questions that could be explored. These will be addressed now.

Governance options

Follow-up research should look into the different governance options described and validated in this research. The next important research step is to look into different IoT device vulnerabilities and research whether these issues are completely resolvable through standardization or informing users. This research only provided the first insights in the next possible steps, while the follow-up research has to look into the different options found in detail. For instance, by saying that informing users is an option: how specifically should these users be informed and what information specifically should be given?

The same goes for standardization and legislation. Future research should look into what exactly this standardization should entail when applied to IoT devices. How should it be enforced? And are the identified issues in IoT devices really solved by enforcing standardization?

Expanding research

Taking on a bigger scope in terms of area and try to map out the problem in more detail by looking at a more comprehensive dataset is also a next research option. This research looked at the area of The Hague, which caused limitations. Using the dataset of The Hague as in indicator that vulnerabilities exist, this research can be expanded to a national level. Such a dataset is not available at the moment, but would be able to give more detailed conclusions from network scan data. Answering questions like: what amount of devices are found? What percentage of devices are vulnerable? Is this number increasing or decreasing? Possibly comparing this with the (average) amount of smart devices sold in the Netherlands could better indicate the scale of IoT vulnerabilities.

Adding stakeholders

Further researching different perspectives from other stakeholders (then defined in this research) will also progress the problem identified. Resulting from the limitations, a study into the role and perspective of IoT device manufacturers would add to this research and would be able to (possibly) provide a different perspective on the identified security issues. What is the perspective of the device manufacturer? What current options do they have and why are they (not) implemented? And how should vulnerabilities be fixed according to this stakeholder? By looking at these questions from a manufacturer's point of view the information could be balanced with the information provided by the ISPs and municipality.

The list of options is not finite and cannot be seen as final. Therefore, the next research steps can look into the possible governance options that might not have been described in this research or literature. This could also add to the collection of governance options provided in this research. By having more stakeholders involved (expanding the research), you could look into the governance options other stakeholders might bring to the table, or governance options that are not addressed in this research.

Bibliography

Abdul-Ghani, H. A., & Konstantas, D. (2019). A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective. *Journal of Sensor and Actuator Networks*, *8*(2), 22. https://doi.org/10.3390/jsan8020022

Abend, G. (2008). The meaning of “Theory.” *Sociological Theory*, *26*(2), 173–199. https://doi.org/10.1111/j.1467-9558.2008.00324.x

Aksnes, D. W., Langfeldt, L., & Wouters, P. (2019). Citations, Citation Indicators, and Research Quality: An Overview of Basic Concepts and Theories. *SAGE Open*, *9*(1). https://doi.org/10.1177/2158244019829575

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. In *Journal of Network and Computer Applications* (Vol. 88, pp. 10–28). Academic Press. https://doi.org/10.1016/j.jnca.2017.04.002

Albada Jelgersma, P. (2020). Wat Internet of Things betekent voor Nederland. *GOV Magazine*, 36–38. https://atos.net/wp-content/uploads/2018/06/atos-btn-nl-gov14.pdf

Alladi, T., Chamola, V., Sikdar, B., & Choo, K. K. R. (2020). Consumer IoT: Security Vulnerability Case Studies and Solutions. *IEEE Consumer Electronics Magazine*, *9*(2), 17–25. https://doi.org/10.1109/MCE.2019.2953740

Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*, 8–27. https://doi.org/10.1016/j.jisa.2017.11.002

Apthorpe, N., Reisman, D., & Feamster, N. (2017). A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. *ArXiv*. http://arxiv.org/abs/1705.06805

Arasteh, H., Hosseinnezhad, V., Loia, V., Tommasetti, A., Troisi, O., Shafie-Khah, M., & Siano, P. (2016, August 29). Iot-based smart cities: A survey. *EEEIC 2016 - International Conference on Environment and Electrical Engineering*. https://doi.org/10.1109/EEEIC.2016.7555867

Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). Proposed embedded security framework for Internet of Things (IoT). *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2011*. https://doi.org/10.1109/WIRELESSVITAE.2011.5940923

Bishop, M. (2003). What is computer security? In *IEEE Security and Privacy* (Vol. 1, Issue 1, pp. 67–69). https://doi.org/10.1109/MSECP.2003.1176998

Borrás, S., & Edler, J. (2014). The governance of change in socio-technical and innovation systems: Three pillars for a conceptual framework. In *The Governance of Socio-Technical Systems: Explaining Change* (pp. 23–48). Edward Elgar Publishing Ltd. https://doi.org/10.4337/9781784710194.00011

Borrás, S., & Edler, J. (2020). The roles of the state in the governance of socio-technical systems’ transformation. *Research Policy*, *49*(5), 103971. https://doi.org/10.1016/j.respol.2020.103971

Brannen, J. (1992). Mixing Methods: qualitative and quantitative research. In *Mixing Methods: qualitative and quantitative research*. Routledge. https://doi.org/10.4324/9781315248813

Brass, I., & Sowell, J. H. (2020). Adaptive governance for the Internet of Things: Coping with emerging security risks. *Regulation & Governance*, rego.12343. https://doi.org/10.1111/rego.12343

Bruines, S. (2018a). *Gemeenten en politie werken samen aan een smart society*. VNG. https://vng.nl/artikelen/gemeenten-en-politie-werken-samen-aan-een-smart-society

Bruines, S. (2018b). Uitvoering NL Smart City Strategie. In *Gemeente Den Haag*. www.denhaag.nl

Bryson, J. M. (2007). *Public Management Review What to do when Stakeholders matter Stakeholder Identification and Analysis Techniques*. https://doi.org/10.1080/14719030410001675722

BSI. (2018). *Information and Cyber Challenges in the Public Sector Survey 2018*.

Carter, N., Bryant-Lukosius, D., Dicenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. In *Oncology Nursing Forum* (Vol. 41, Issue 5, pp. 545–547). Oncology Nursing Society. https://doi.org/10.1188/14.ONF.545-547

Cetin, O., Ganan, C., Altena, L., Kasama, T., Inoue, D., Tamiya, K., Tie, Y., Yoshioka, K., & Van Eeten, M. (2019). *Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai*. https://doi.org/10.14722/ndss.2019.23438

Cetin, O., Ganan, C., Altena, L., Tajalizadehkhoob, S., & Van Eeten, M. (2019). Tell me you fixed it: Evaluating vulnerability notifications via quarantine networks. *Proceedings - 4th IEEE European Symposium on Security and Privacy, EURO S and P 2019*, 326–339.

https://doi.org/10.1109/EuroSP.2019.00032
DCMS. (2018). *Code of Practice for Consumer IoT Security*. https://www.gov.uk/government/publications/secure-by-design
De Carli, L., & Mignano, A. (n.d.). *Network Security for Home IoT Devices Must Involve the User: a Position Paper*.
DeNardis, L. (2020). *The Internet in Everything* . Yale University Press. https://books.google.nl/books?hl=nl&lr=&id=gy7EDwAAQBAJ&oi=fnd&pg=PP1&dq=The+Internet+in+Everything:+Freedom+and+Security+in+a+World+with+No+Off+Switch&ots=HZ-9m3x6t_&sig=ru0lb_hv9nV7fsme2FXvriAKG7M#v=onepage&q=The Internet in Everything%3A Freedom and Security in a World with No Off Switch&f=false
Dicicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical Education*, *40*, 314–321. https://doi.org/10.1111/j.1365-2929.2006.02418.x
Dutton, W. H. (2014). Putting things to work: Social and policy challenges for the Internet of things. *Info*, *16*(3), 1–21. https://doi.org/10.1108/info-09-2013-0047
Emami-Naeini, P., Dixon, H., Agarwal, Y., & Cranor, L. F. (2019). Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. *CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019)*, *12*(2019). https://doi.org/10.1145/3290605.3300764
ETSI. (2020). *Cyber Security for Consumer Internet of Things: Baseline Requirements* (Vol. 1, pp. 1–34). https://doi.org/EN 303 645 - V2.1.1 -
Principles relating to processing of personal data, Article 5, General Data Protection Regulation (GDPR) (2016). https://gdpr-info.eu/art-5-gdpr/
Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). *Foundational Cybersecurity Activities for IoT Device Manufacturers*. https://doi.org/10.6028/NIST.IR.8259
Fossey, E., Harvey, C., McDermott, F., & Davidson, L. (2002). Understanding and evaluating qualitative research. *Australian and New Zealand Journal of Psychiatry*, *36*(6), 717–732. https://doi.org/10.1046/j.1440-1614.2002.01100.x
Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of Things Journal*, *5*(4), 2483–2495. https://doi.org/10.1109/JIOT.2017.2767291
Gemeente Den Haag. (2021). *Digitaal Den Haag*. Gemeente Den Haag. https://www.denhaag.nl/nl/bestuur-en-organisatie/projecten-en-themas/digitaal-den-haag.htm
Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M., & Al-Fuqaha, A. (2017). Smart Cities: A Survey on Data Management, Security, and Enabling Technologies. In *IEEE Communications Surveys and Tutorials* (Vol. 19, Issue 4, pp. 2456–2501). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/COMST.2017.2736886
Granjal, J., Monteiro, E., & Sa Silva, J. (2015). Security for the internet of things: A survey of existing protocols and open research issues. *IEEE Communications Surveys and Tutorials*, *17*(3), 1294–1312. https://doi.org/10.1109/COMST.2015.2388550
Grapperhaus, F., van Toorenburg, M., & Verhoeven, K. (2018). Antwoord op vragen van de leden Van Toorenburg en Verhoeven over het bericht ‘Experts: overheid moet ingrijpen bij internetapparaten.’ *Aanhangsel van de Handelingen - Vragen Gesteld Door de Leden Der Kamer, Met de Daarop Door de Regering Gegeven Antwoorden*, 1–3. https://www.tweedekamer.nl/downloads/document?id=3ec6034f-51c8-40cc-8b62-ae539eb53e46&title=Antwoord op vragen van de leden Van Toorenburg en Verhoeven over het bericht ‘Experts%3A overheid moet ingrijpen bij internetapparaten’.pdf
Guo, H., & Heidemann, J. (2018). IP-Based IoT device detection. *IoT S and P 2018 - Proceedings of the 2018 Workshop on IoT Security and Privacy, Part of SIGCOMM 2018*, 36–42. https://doi.org/10.1145/3229565.3229572
Gupta, K., & Shukla, S. (2016). Internet of Things: Security challenges for next generation networks. *2016 1st International Conference on Innovation and Challenges in Cyber Security, ICICCS 2016*, 315–318. https://doi.org/10.1109/ICICCS.2016.7542301
Hammi, B., Khatoun, R., Zeadally, S., Fayad, A., & Khoukhi, L. (2018). IoT technologies for smart cities. In *IET Networks* (Vol. 7, Issue 1, pp. 1–13). Institution of Engineering and Technology. https://doi.org/10.1049/iet-net.2017.0163
Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. In *IEEE Access* (Vol. 7, pp. 82721–82743). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2019.2924045

Hay Newman, L. (2016). ISPs Could Be the Key to Securing Existing IoT Devices. *WIRED*. https://www.wired.com/2016/10/internet-providers-key-securing-iot-devices-already/
Hay Newman, L. (2021, April 13). 100 Million More IoT Devices Are Exposed—and They Won't Be the Last . *WIRED*. https://www.wired.com/story/namewreck-iot-vulnerabilities-tcpip-millions-devices/
Herr, T., Kim, N., & Scheier, B. (2021). Cyber insurance and private governance: The enforcement power of markets. *Regulation and Governance*, *15*(1), 98–114. https://doi.org/10.1111/rego.12266
Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. *Proceedings - 2015 IEEE World Congress on Services, SERVICES 2015*, 21–28. https://doi.org/10.1109/SERVICES.2015.12
Hsu, C. L., & Lin, J. C. C. (2016). An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behavior*, *62*, 516–527. https://doi.org/10.1016/j.chb.2016.04.023
IT Governance Institute. (2013). *Definition of Governance*. Oxford Dictionary. https://www.lexico.com/definition/governance
ITU-T. (2012). Y.2060 An overview of internet of things. In *SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS*.
Jaquith, A. (2007). *Security Metrics: Replacing Fear, Uncertainty, and Doubt* (1st ed.). Addison-Wesley Professional.
Jayawardane, S., Larik, J., & Jackson, E. (2015). *Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance Sash Jayawardane*.
Kate Conger, Richard Fausset, & Serge F. Kovaleski. (2019). San Francisco Bans Facial Recognition Technology. *The New York Times*. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html
Keijzer, M. C. G. (2020). Voortgang Roadmap Digitaal Veilige Hard- en Software. *Informatie- En Communicatietechnologie (ICT) - Brief Regering;*, *26 643*, nr. *735*, 1–9. https://doi.org/735
Kotz, D., & Peters, T. (2017). Challenges to ensuring human safety throughout the life-cycle of Smart Environments. *SafeThings 2017 - Proceedings of the 1st ACM International Workshop on the Internet of Safe Things, Part of SenSys 2017*, 1–7. https://doi.org/10.1145/3137003.3137012
Kuerbis, B., & Badiei, F. (2017). Mapping the cybersecurity institutional landscape. *Digital Policy, Regulation and Governance*, *19*(6), 466–492. https://doi.org/10.1108/DPRG-05-2017-0024
Lampe, J. (2014, November 10). *How to Test the Security of IoT Smart Devices - Infosec Resources*. INFOSEC. https://resources.infosecinstitute.com/topic/test-security-iot-smart-devices/
Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431–440. https://doi.org/10.1016/j.bushor.2015.03.008
Levy-Bencheton, C. (2018). *White Paper Incentives for IoT Security*.
Loi, F., Sivanathan, A., Gharakheili, H. H., Radford, A., & Sivaraman, V. (2017). Systematically evaluating security and privacy for consumer IoT devices. *IoT S and P 2017 - Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, Co-Located with CCS 2017*, 1–6. https://doi.org/10.1145/3139937.3139938
Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2016). Internet of things (IoT) security: Current status, challenges and prospective measures. *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, 336–341. https://doi.org/10.1109/ICITST.2015.7412116
Marky, K., Voit, A., Stöver, A., Kunze, K., Schröder, S., & Mühlhäuser, M. (2020, October 25). "I don't know how to protect myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3419249.3420164
Mehmood, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M., & Guizani, S. (2017). Internet-of-Things-Based Smart Cities: Recent Advances and Challenges. *IEEE Communications Magazine*, *55*(9), 16–24. https://doi.org/10.1109/MCOM.2017.1600514
Melzer, J., Latour, J., Richardson, M., Ali, A., & Almuhtadi, W. (2020). Network approaches to improving consumer IoT security. *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, *2020-January*. https://doi.org/10.1109/ICCE46568.2020.9043121
Merriam, S. B., & Tisdell, E. J. (2015). *Qualitative Research: A Guide to Design and Implementation* (4th ed.). Jossey-Bass | Wiley. https://www.wiley.com/en-ae/Qualitative+Research%3A+A+Guide+to+Design+and+Implementation%2C+4th+Edition-p-9781119003618
Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and

research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516. https://doi.org/10.1016/j.adhoc.2012.02.016
Mueller, M., Schmidt, A., & Kuerbis, B. (2013). Internet security and networked governance in international relations. *International Studies Review*, *15*(1), 86–104. https://doi.org/10.1111/misr.12024
Ning, H., & Liu, H. (2012). Cyber-Physical-Social Based Security Architecture for Future Internet of Things. *Advances in Internet of Things*, *02*(01), 1–7. https://doi.org/10.4236/ait.2012.21001
NIST. (2015). *Cyber threat*. 2–3. https://csrc.nist.gov/glossary/term/Cyber_Threat
NVD - CVE-2010-5298. (n.d.). Retrieved May 13, 2021, from https://nvd.nist.gov/vuln/detail/CVE-2010-5298
Palmer, D. (2021). This old security vulnerability left millions of Internet of Things devices vulnerable to attacks. *ZDnet*. https://www.zdnet.com/article/this-old-security-vulnerability-left-millions-of-internet-of-things-devices-vulnerable-to-attacks/
Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Sensing as a service model for smart cities supported by Internet of Things. *Transactions on Emerging Telecommunications Technologies*, *25*(1), 81–93. https://doi.org/10.1002/ett.2704
Pishcva, D., & Takeda, K. (2006, October). Product-Based Security Model for Smart Home Appliances. *IEEE A&E SYSTEMS MAGAZINE*, 32–41. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4665323&casa_token=GsKhyP8DcoYAAAAA:GhM6S14carfkR_pemm40jzXp7-nUdLq6XEXGYcNwVErmuNUph5YF691nMtzYHOGgTwFHClAk
Popay, J., Rogers, A., & Williams, G. (1998). Rationale and standards for the systematic review of qualitative literature in health services research. In *Qualitative Health Research* (Vol. 8, Issue 3, pp. 341–351). SAGE Publications Inc. https://doi.org/10.1177/104973239800800305
Press, G. (2015). *A Very Short History Of The Internet And The Web*. Forbes. https://www.forbes.com/sites/gilpress/2015/01/02/a-very-short-history-of-the-internet-and-the-web-2/?sh=37f9efb47a4e
Qu, S., & Dumay, J. (2011). *The Qualitative Research Interview*. https://papers-ssrn-com.tudelft.idm.oclc.org/abstract=2058515
Quach, K. (2018). *Default Username and Password in Internet of Things*. https://www.diva-portal.org/smash/get/diva2:1252229/FULLTEXT01.pdf
Radanliev, P., De Roure, D., Maple, C., Nurse, J. R. ., Nicolescu, R., & Ani, U. (2019). Cyber Risk in IoT Systems. *University of Oxford Combined Working Papers and Project Reports Prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre*, *169701*(2017), 1–27. https://doi.org/10.20944/preprints201903.0104.v1
Riahi Sfar, A., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*(2), 118–137. https://doi.org/10.1016/j.dcan.2017.04.003
Roman, R., Najera, P., & Lopez, J. (2011). Securing the Internet of things. *Computer*, *44*(9), 51–58. https://doi.org/10.1109/MC.2011.291
Roscia, M., Longo, M., & Lazaroiu, G. C. (2013). Smart City by multi-agent systems. *Proceedings of 2013 International Conference on Renewable Energy Research and Applications, ICRERA 2013*, 371–376. https://doi.org/10.1109/ICRERA.2013.6749783
Ruijgh, T., van Daalen, E., Bots, P., Steenhuisen, B., Janssen, M., Warnier, M., Lukosch, S., van der Voort, H., & Bouwmans, I. (2019). *Designing in socio-technical systems* (1st ed.). Faculty of Technology, Policy and Management, Delft University of Technology.
Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2016). Twenty security considerations for cloud-supported Internet of Things. *IEEE Internet of Things Journal*.
Smart City Den Haag . (n.d.). Gemeente Den Haag. Retrieved March 30, 2021, from https://smartcity.denhaag.nl/
SSL Support Team. (2019, October 2). *What is SSL?* SSL.Com. https://www.ssl.com/faqs/faq-what-is-ssl/
Stahie, S. (2020). Why Vulnerable IoT Is a Double-Sided Problem for ISPs and Their Customers. *Security Boulevard*. https://securityboulevard.com/2020/07/why-vulnerable-iot-is-a-double-sided-problem-for-isps-and-their-customers/
Talari, S., Shafie-Khah, M., Siano, P., Loia, V., Tommasetti, A., & Catalão, J. P. S. (2017). A review of smart cities based on the internet of things concept. In *Energies* (Vol. 10, Issue 4, p. 421). MDPI AG. https://doi.org/10.3390/en10040421
Directive 2014/53/EU of the European Parliament and of the Council , EUR-Lex (2018). http://data.europa.eu/eli/dir/2014/53/oj
The Hague Security. (2020). How to Make People Aware of Cyber Risks in a Fun Way. *The Hague Security Delta*. https://www.thehaguesecuritydelta.com/news/newsitem/1597-how-to-make-people-aware-of-

cyber-risks-in-a-fun-way
United States Government. (1998). Limitations on Liability Relating to Material Online. *US Law*, *512*(March), 1–13. https://www.law.cornell.edu/uscode/text/17/512
Van Eeten, M. (2017). Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. *Digital Policy, Regulation and Governance*, *19*(6), 429–448. https://doi.org/10.1108/DPRG-05-2017-0029
Van Eeten, M. J., Bauer, J. M., Asghari, H., Tabatabaie, S., & Rand, D. (2010). The Role of Internet Service Providers in Botnet Mitigation An Empirical Analysis Based on Spam Data. *Development*, *May 2014*, 1–31. http://weis2010.econinfosec.org/program.html
Visterin, W. (2016, January 27). IoT en security: deze beelden zeggen genoeg. *Computable.Nl*. https://www.computable.nl/artikel/columns/security/5692122/1509086/iot-en-security-deze-beelden-zeggen-genoeg.html
Wachter, S. (2018). The GDPR and the internet of things: A three-step transparency model. *Law, Innovation and Technology*, *10*(2), 266–294. https://doi.org/10.1080/17579961.2018.1527479
Wahab, A., Ahmad, O., Muhammad, M., & Ali, M. (2017). A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT. *International Journal of Advanced Computer Science and Applications*, *8*(7). https://doi.org/10.14569/ijacsa.2017.080768
Weber, R. H. (2009). Internet of things - Need for a new legal environment? *Computer Law and Security Review*, *25*(6), 522–527. https://doi.org/10.1016/j.clsr.2009.09.002
Weber, R. H. (2013). Internet of things - Governance quo vadis? *Computer Law and Security Review*, *29*(4), 341–347. https://doi.org/10.1016/j.clsr.2013.05.010
Zeng, E., Mare, S., Roesner, F., & Allen, P. G. (2017). *End User Security and Privacy Concerns with Smart Homes End User Security & Privacy Concerns with Smart Homes*. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng
Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine*, *55*(1), 122–129. https://doi.org/10.1109/MCOM.2017.1600267CM
Zhao, K., & Ge, L. (2013). A survey on the internet of things security. *Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013*, 663–667. https://doi.org/10.1109/CIS.2013.145
Zheng, S., Apthorpe, N., & Feamster, N. (2018). User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact*, *2*, 20. https://doi.org/10.1145/3274469

Appendix

Appendix A: The knowledge gap

Table A.1. An overview of the 18 sources of literature used.

Authors:	Title:	Relevant finding:	Relevant knowledge gap:
Gupta & Shukla, 2016	Internet of Things: Security challenges for next generation networks	Privacy is a challenge in IoT	Solving through monitoring every device, which is not permitted.
Alaba et al., 2017	Internet of Things security: A survey	Managing IoT is difficult	The combination of protocols and rules is missing in current IoT developments
Zhao & Ge, 2013	A Survey on the Internet of Things Security	Managing IoT is difficult	Lack of specificity on how to solve or design solutions.
Babar et al., 2011	Proposed embedded security framework for Internet of Things (IoT)	Lack of standardization causes security issues	Lack of specificity on how to solve or design standardization, and for which IoT devices
Miorandi et al., 2012	Internet of things: Vision, applications and research challenges	Design IoT with security in mind at every step	The need for standardization
Singh et al., 2016	Twenty security considerations for cloud-supported Internet of Things	There is a lack of governance relating to cloud-based IoT	Specifics of governance not known
Hossain et al., n.d.	Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things	Governance can solve security but also cause issues like privacy	Solving issues governance causes is not specified
Hsu & Lin, 2016	An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives	Users are indifferent or unaware of any privacy infringement.	Reaching users and creating more security and privacy awareness.
Marky et al., 2020	"I don't know how to protect myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments	Users are indifferent or unaware of any privacy infringement, and bystanders should be informed.	Reaching users and creating more security and privacy awareness.
Zeng et al., 2017	End User Security and Privacy Concerns with Smart Homes End User Security & Privacy Concerns with Smart Homes	Privacy awareness is lacking among users	How to make users more aware of security and privacy issues
Loi et al., 2017	Systematically evaluating security and privacy for consumer IoT devices	Security needs to be addressed through standards from policymakers, legislators, and the industry itself	The lack is shown, but how do you solve this, and what would this governance entail.
Tejasvi Alladi et al., 2020	Consumer IoT: Security Vulnerability Case Studies and Solutions	Timely updates will solve software vulnerabilities	How do you get users to update their device
Pishcva & Takeda, 2006	Product-Based Security Model for Smart Home Appliances	Many issues that need a specific actor to solve it: software vulnerabilities are a practical problem	How do you prevent software vulnerabilities by educating R&D, and how do you educate users on these vulnerabilities.
Emami-Naeini et al., 2019	Exploring How Privacy and Security Factor into IoT Device Purchase Behavior	Users don't look into security information but value security.	How to make users more involved in security and privacy issues and have them perform updates
Cetin, Ganan, Altena, Kasama, et al., 2019	Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai	Remediation by users can be successful. ISPs have weak incentives to act.	How to inform users better (and educate them; wrong mental model). What data should be used by what stakeholder?
Cetin, Ganan, Altena, Tajalizadehkhoob, et al., 2019	Tell Me You Fixed It: Evaluating Vulnerability Notifications via Quarantine Networks	A lack of identification of device owners, communication channels to these owners, and actionable notifications	Quarantining is effective but can not be deployed as a general internet-wide solution because of lacking user information
De Carli & Mignano, n.d.	Network Security for Home IoT Devices Must Involve the User: a Position Paper	Research on IoT security techniques should involve and be aware of the user.	What novel forms of communication of security findings should be used.

Appendix B: Device findings from the network scan data

Table A.2. The types of devices and brands identified from the dataset.

Technology		**Brand**	**Total number in dataset**
Webcam		*A*	6
		B	5
		C	5
		D	6
		E	7
		F	2
		G	7
Router		*H*	46
		I	37
		J	2
		K	7
		L	2
		M	2
		N	3
Hard drives		*O*	47
Home management IoT	Energy and household	*P*	4
	Smart lighting	Q	3
			191

Appendix C: Findings on internet service providers and device types.

The ISPs and other companies found are anonymized since mentioning them is not required for this research. The different types of devices found at each identified ISP is mentioned, as well as a description of the type of ISP and the customers they serve. For five devices it was unclear to determine the ISP involved, these are mentioned as well.

Table A.3 The different ISPs and devices at these providers identified from the dataset.

	Type of device	**ISP description**
1	9 H brand routers, 1 D brand webcams, 3 Q brand lighting, 2 A brand webcam, 22 I brand routers, 25 O brand hard drives, 6 E brand webcams, 4 P brand energy and household, 2 F webcams, 2 G brand webcams, 2 M brand routers, 3 N brand routers	Growing medium-big sized consumer-oriented provider. Focuses on high-speed internet.
	9 H brand routers	Growing medium-sized provider-oriented towards businesses. Focuses on high-speed internet.
2	3 H brand routers	Small business-oriented provider
3	10 H brand routers, 2 O brand hard drives, 2 D brand webcams, 1 E brand webcam 2 L brand routers	Prominent large sized all-around consumer and business provider, with security department.
4	2 H brand routers, 2 J brand router	Medium-sized business ISP with a focus on speed and controlling the network.
5	2 H brand routers	Medium-sized business ISP that's part of an international ISP.
6	3 H brand routers	Small business-oriented ISP.
7	4 A brand webcams, 5 C brand webcams, 4 H brand routers, 15 I brand routers, 20 O brand hard drives, 3 D brand webcams, 5 G brand webcams, 1 K brand routers	Big all-round consumer and business-oriented provider, with security department
8	6 K brand routers	Locally set up ISP to provide internet to local businesses
9	4 H brand routers	Two companies setting up and acting as their own ISP
Total:	186	

Unclear what ISP is involved		
	Type of device	**Company description**
	2 B brand webcams	Business-oriented IT service provider, medium-sized, providing cloud access for its clients. Focusses' on security.
	2 B brand webcams	Well-known technology brand that hosts the web interface linked to their IoT devices.
	1 B brand webcams	Small-medium sized business IT service provider that hosts the web interface belonging to the IoT device.
Total:	5	

Table A.4. A similar overview as A.3, but focussing on amount of devices for each provider.

	Device manufacturer:																
Provider:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	**Total devices:**
1	2	-	-	1	6	2	2	18	22	-	-	-	2	3	25	4	3	90
2	-	-	-	-	-	-	-	3	-	-	-	-	-	-	-	-	-	3
3	-	-	-	2	1	-	-	10	-	-	-	2	-	-	2	-	-	17
4	-	-	-	-	-	-	-	2	-	2	-	-	-	-	-	-	-	4
5	-	-	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	2
6	-	-	-	-	-	-	-	3	-	-	-	-	-	-	-	-	-	3
7	4	-	5	3	-	-	5	4	15	-	1	-	-	-	20	-	-	57
8	-	-	-	-	-	-	-	-	-	-	6	-	-	-	-	-	-	6
9	-	-	-	-	-	-	-	4	-	-	-	-	-	-	-	-	-	4
																Total:		186

	Uncertain what ISP is involved:																	
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	**Total devices:**
	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2
	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2
	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1
																Total:		5

Appendix D: Information sheet provided to participants

This information sheet was provided to the participants before the interviews were conducted, to inform them about the interview intentions and the research. Also to inform them about how their data will be used and stored.

Information sheet:
This interview will be part of the master thesis research for the Complex Systems engineering and Management master at the Technische Universiteit in Delft.

Research description:
Connecting devices to the internet, known as 'the Internet of Things' (IoT), increases the amount of smart objects. With innovations and uses in the area of IoT increasing (e.g. smart cities) this leads to a growing chance of security incidents (leaking of privacy sensitive information, hacking of devices, vulnerable devices etc.). For this research there is a dataset with network scan data on IoT devices in The Hague. For these devices it contains information on brand, vulnerabilities, and internet services provider. These could be webcams or routers, from which you can access the login page from outside of the network the device is part of. In combination with unsafe security practices (like default passwords for instance) such a device can become a security risk (hackers, for instance).
Most vulnerabilities in these devices can be solved by reaching the right person (stakeholder) and taking action. For instance internet service providers or manufacturers of these IoT devices. Reaching the right stakeholder can be done through governance options: rules, regulations, social interactions, or any 'mechanism' used to manage or govern IoT. What actions can be taken and why these actions are not taken and by what stakeholder is unclear at the moment. This research is aimed at finding out what stakeholders are involved, how they look at the problem and what role they play, and what they can do in terms of governance options.

How will this interview be used?
By using IoT network scan data of The Hague IoT devices can be identified. The identified stakeholders from this data for this research are device manufacturers, internet service providers, and the municipality. These stakeholders can implement different governance options (rules, agreements, regulations, guidelines etc.) to make IoT devices safer. However, to find out what roles and perceptions these stakeholders have, and what is in their way of the 'ideal' situation the options derived from the IoT data will have to be validated. This interview will provide that expert validation.

Objective:
The research objective will be finding the most suitable governance options and the criteria or barriers for implementation. The purpose of this research is to provide a real world context to the described vulnerable IoT devices, by using network scan data of the area of The Hague. By participation in this research you validate or criticise information found through literature and data analysis, by giving your expert opinion or view on the information presented. No personal information will be gathered.

The risk of participating in this research is showing the perspective or view your organization has about the problem described in the research description. To minimize this chance your interview will be anonymized, meaning that no name will be used and you will be generalized in the research as*: "According to an Internet service provider… ", "the municipality",* or: *"A manufacturer of IoT devices"* for instance.

By participating in this research you provide insight about the real world context in which the problem exists as described in the research description. The main findings of these interviews will be reflected in the master research project, and used to provide backing to findings from the IoT dataset used as well as literature analyzed.

Gathering of information:
No personal information of the participants will be collected during the interviews. Only the name of the participant and the organization he/she represents will be temporarily stored during the research, but not used in the research itself.
Your responses and the information you provide will be used as input for research questions. The option will be provided to make statements anonymously. The interview will be recorded as a video locally, and then be transcribed. This transcript will be shared with the participant for approval.

The nature of this research is exploratory and therefore there is no clear set of information needed to be acquired during these interviews. The expert validations are used to provide insights in the identified research problem for the 'real world'.

Storage:
The interview data (consisting of the recorded video of the interview, transcript, and consent form) will be stored on a password protected TU Delft drive that is only accessible to named researchers involved in the project. Access to the data by the participant is available upon request to the researcher and his supervisors. The interview will be stored in a subfolder per participant with the data consisting of: a video or audio recording of the interview, an interview transcript, and this signed consent form. This interview data will be stored until the master research is graded and published in the TU Delft repository for research, after which the full interview data will be deleted. No data will be interview data will be used or made available for other research, the findings from these interviews will only be used in this specific master thesis research.

Withdrawal:
In case the participant does not agree to the research before, during, or after the interview; or in case the participant does not agree with the shared transcript of their interview they are able to withdraw from participating at any time. To do this please contact the researcher.

Appendix E: Interview protocol

This interview protocol is used for the semi-structured interviews, to guide the conversation and ensure information concerning the right topics was gained from the interviews. The participant could talk freely and add information or bring up points themselves, this protocol was used as a guide. The governance options described in this protocol depend on the interviewee (what stakeholder), and were used as probes to see why a stakeholder might not be able to implement the defined options.

---

1. Do you perceive any challenges around the following information?
Providing findings from the data to see how the participant perceives this situation, and if they think it is a problem or not.

- Information from dataset:
→1649 IP addresses in the area of The Hague
- Geographic location non-specific, and also from other places.
- Only ISP's and devices identifiable from IP address.

→ 191 IoT devices identified through a login web interface:
→ **Webcams**: 38
→ **Routers**: 99
→ **Hard drives:** 47
→ **Smart home IoT devices**:→ Energy management: 4
→ Smart lighting: 3

- Explain that vulnerabilities for users that could result in security issues for the entire network.

Follow-up: **Do you think this is something that should be fixed?**
→ *Does it feel urgent? Why (not)?*

2. Who should solve this according to you?
→ *Who is responsible to solve this?*
→ *Do you have a role in this?*

3. How would you, as stakeholder x, be able to do option y?
Present the different options (depending on the interviewee):

Manufacturers	→ *Security-by-design*
ISP or municipality	→ *Steering manufacturers*
Examples: Enforcing through legislation, Creating standards, Security labels, Only secure devices allowed	
ISP or municipality	→ *Steering device users*
Examples: Security labels, Only secure devices allowed, Discounting 'secure' devices	
Manufacturer, ISP, Municipality	→ *Informing device users*
Examples: Send out a letter/email to say IoT devices can be vulnerable, Campaign about IoT security, Provide helpdesk service for secure IoT configuration and usage	
Municipality	→ *Steering ISPs*
Examples: Forcing ISPs to contact vulnerable device users	
Municipality, ISPs	→ *Policing IoT*
Examples: Going door-to-door to check vulnerabilities and solve them, Force people to update their device or get a new one.	

(Potential) follow-up: **How feasible would these options be for you?**

4. What is keeping you, stakeholder x, from doing option y?

Examples for the conversation, resulting from expectations and literature:

- *Legal reasons?*
- *(Technical) knowledge?*
  → *For instance*: Setting up helpdesk, thinking of standards, 100% secure is not possible.
- Having information on the situation?
  → *For instance:* the amount of IoT devices, what vulnerabilities, problem increasing etc.
- Involvement of others?
  → *For instance:* Collaboration between stakeholders, if others get involved, would the options change?

5. What would you require in order to take action?

- Are there things that could be changed now for you to take action? → 'Requirements'
  → Does it depend on other stakeholders?

Appendix F: Short interview report

The interviews were semi-structured to have participants be able to add information or conversation points that might not be included in the interview protocol. All three ISP representatives started by explaining how an IoT device connects to the internet through their networks, and what services they do and do not offer on this. This automatically gave in indication of their perspective on IoT. During the interviews all three ISPs told a similar story, explained what their company does and what they value, and stated that ISPs are network facilitators that do not want to actively check on customers.

After this start of the conversations the interview protocol was followed or referenced as a guideline, and the findings from the dataset were communicated to the interview. This added to the point of being a network facilitator, since all three ISPs said that vulnerabilities seemed like a problem, but it was only a problem for single users and therefore not for the ISP. After this some governance options were brought up and discussed, with the ISPs giving similar reasons why most options will not work: legal boundaries, lack of a business case, or not their role to play. Some ISPs even had attempted options in the past, and therefore knew they would not work. This part of the conversation mostly resulted in examples by the interviewees why certain options would not work and explaining their view on this.

The interview with the municipality representative was guided more by the interview protocol since the representative was aware of Cybersprint and the data collection. Therefore the interviewee indicated that the findings from the data were recognized as a problem and that it feels the municipality should play a role, while at the same time saying it was uncertain what role. After explaining their perspective and the role ISPs or manufacturers should have, a few different governance options applicable to the municipality were brought up. Here it became clear that the role of the municipality is not in actively solving vulnerabilities, but in leading other actors into solving this problem. This concluded the conversation.

Appendix G: The collection of governance options.

Table A.5. All governance options defined for this research.

Security-by-design	
	1. Force two-factor authentication to log in.
	2. Force mandatory password changes (from default) before usage.
	3. Force mandatory password changes every set number of days.
	4. Store sensitive credentials encrypted on the device or service
	5. Force automatic software updates
	6. Enforce the principle of least privilege: restrict users' rights and services to only the functionalities they need.
	7. Provide clear insights to the user how their data is being used (according to GDPR)
	8. Let devices periodically send a diagnostic status report to the device manufacturer for inspection.
	9. Let the device notify the device owner when the device interface is (attempted) to be accessed.
	10. Set up a factory reset option that locks a device, cleans it up, brings back default values, and has a helpdesk to set up the device safely.
	11. Use state of the art technology as a standard.
	12. Force timely, automatic software updates.
	13. Ensure the latest software version is installed before the device is being sold.
	14. Design devices to operate exclusively on private networks, and if remote management is needed, have this communication encrypted.
	15. Enable the function to lock the device and provide a guide to configure the device every time the device is reset safely.
	16. Physically make wrong configurations through hardware impossible.
	17. Enable a lock function that locks a device if a user attempts to use the device for other intended purposes.
	18. Once a security issue is detected, a device gets locked and is only usable again through owner verification and guided secure setup through a helpdesk.
	19. Enforce coordinated vulnerability disclosures to let vulnerabilities be researched
	20. Invest in security through the acquisition of investors by promoting security aspects of your products.
	87. Enable devices to reset themselves if the service or device is not used in an x number of days.
	88. Reset user passwords if the service or device has not been used in an x number of days.
Steering manufacturers	
	21. Only allow devices that live up to specific security standards onto the network.
	22. Agree with manufacturers to give out only their IoT devices to ISP customers if the manufacturer ensures specific security standards are followed.
	33. Make agreements with specific manufacturers to manufacture devices that live up to the current level of technology and security levels.
	34. Provide manufacturers with financial compensation to sell a more secure device for lower prices and devices that are less secure for higher prices.
	35. Require manufacturers to add a security label or security information to the device to inform users about potential vulnerabilities before buying.
Steering manufacturers	
	23. Make agreements with specific manufacturers to manufacture devices that live up to the current level of technology and security levels.
	24. Agree with manufacturers to give out their IoT devices to citizens (as a municipality) if the manufacturer ensures specific security standards are followed.
	25. Force manufacturers to make devices that follow the highest security standards
	26. Provide manufacturers with financial means to increase the level of security in their IoT devices
	75. Use a ‘three strikes and you are out’ principle, following from the data in networks. If a device manufacturer repeatedly shows up, the manufacturer will be banned from the networks after three ‘strikes’.
Steering ISPs	
	27. Force ISPs to only allow devices that live up to specific security standards onto the network.

	78. Have public networks scanned and find the ISPs belonging to vulnerable devices: then force these ISPs to contact the device owners belonging to these devices.
	85. Pressure ISPs to do a device cleanup in terms of vulnerabilities
	86. Have public networks scanned and find the ISPs belonging to vulnerable devices: then force these ISPs to contact the device owners belonging to these devices.
Steering device users	
	28. Only allow devices to be used that live up to the current technology and security levels.
	44. Give out devices to ISP customers that the ISP approves as being secure.
	45. Do not allow other devices than the devices approved or supplied by the ISP onto the network.
Steering device users	
	40. Only allow devices to be used that live up to the current level of technology and security levels.
	41. Force device vendors to only sell devices that live up to a specific security standard.
	42. Provide device vendors with financial compensation to sell a device that is more secure for lower prices and devices that are less secure for higher prices
	43. Provide users with discounts for specific devices that are the safest options.
	50. Force users to call a helpdesk before being able to set up their device safely
	51. Require the device to be configured by an expert provided by the manufacturer.
	53. Force users to call a helpdesk before being able to set up their device safely.
	54. Require the device to be configured by an expert provided by the Internet Service Provider.
	58. Require the device to be configured by an expert provided by the municipality.
	89. Buy old/not used IoT devices from users.
	90. Give discounts on new IoT devices when users hand in old devices.
	91. Setup a collection point for customers to dispose of their IoT devices to ensure safe disposal/reset of these devices.
	92. Buy old/not used IoT devices from users.
	93. Give discounts on new IoT devices when users hand in old devices.
	95. Setup a collection point for customers to dispose of their IoT devices to ensure safe disposal/reset of these devices.
	96. Buy old/not used IoT devices from users
	97. Give discounts on new IoT devices when users hand in old devices.
	98. Go door-to-door and force users to upgrade their device to a new model
	99. Setup a device selling website the lets users give their IoT device, have it updated and brought to the highest security standards, and then sold to other users.
Informing device users	
	29. Add a security label or security information to the device packaging to inform users about potential vulnerabilities before buying.
	30. Place a notification of potential vulnerabilities or misconfigurations on the device manufacturer website.
	31. Set up a helpdesk to give users the ability to call if users believe their (new) device might be at risk.
	32. Give the warranty to users to swap ‘infected’ devices with new devices (through vendors or manufacturer)
	37. Set up a campaign to advise users on what makes a safe device and what to look for when buying an IoT device.
	38. Setup a security label as a municipality that indicates how secure a device is.
	39. Set up a website where customers can check how secure a device is before buying/acquiring it.
	46. Setup a security label as ISP that indicate how secure a device is
	47. Set up a website where customers can check how secure a device is before buying/acquiring it.
	48. Provide advice on using certified devices to customers to ensure security.
	49. Setup a helpdesk to help users set up their device (manufacturer)
	52. Setup a helpdesk to help users set up their device (internet service provider)
	55. Setup a helpdesk to help users set up their device (municipality)
	56. Set up a campaign to inform users on how to configure their device and what to keep in mind in terms of security.
	57. Send out a letter to every citizen informing them of IoT safety and configuration.
	60. Scan networks for vulnerable or misconfigured IoT devices and reach out to device owners to notify them about security risks found.
	61. Go door-to-door at ISP customers to check whether there are IoT devices misconfigured

	64. Inform citizens in general about potential misconfigured IoT devices they might own and have them contact the manufacturer or vendor.
	65. Go door-to-door to check whether there are IoT devices misconfigured
	67. Place a notification of potential vulnerabilities or misconfigurations on the device manufacturer website.
	68. Place a notification of potential vulnerabilities or misconfigurations on the primary device interface or webpage.
	69. Set up a campaign that shows people how to use an IoT device safely.
	70. Send out a letter to every citizen, informing them of IoT safety and configuration.
	71. Setup a campaign that informs customers how to use an IoT device safely.
	72. Scan networks for vulnerable or misconfigured IoT devices and reach out to device owners to notify them about security risks found.
	73. Set up a helpdesk to give users the ability to call if they believe their device might be at risk.
	74. Go door-to-door at ISP customers to check whether there are IoT devices used and configured insecurely.
	76. Inform citizens in general about potential misconfigured IoT devices they might own and have them contact the manufacturer or vendor.
	77. Go door-to-door to check whether there are IoT devices misconfigured
	79. Set up a helpdesk that provides users with a manual or guidelines on how to remediate the security issues found on their device.
	80. Provide users with a manual or guidelines on how to remediate the security issues found on their device.
	81. Place an up to date guide on how to remediate the security issues found on the manufacturer's device.
	82. Provide users with a manual or guidelines on how to remediate the security issues found on their device.
Policing IoT	
	36. Setup an IT department that inspects and checks devices being sold.
	59. Give out certificates that officially state a device is configured securely.
	62. Go door-to-door at ISP customers to check whether IoT devices are misconfigured and solve issues on the spot.
	63. Only allow IoT devices to be used through a VPN tunnel.
	66. Go door-to-door to check whether there are IoT devices misconfigured and solve issues on the spot.
	83. Quarantine a user device when a security issue is found, only to be taken out of quarantine once the security issue is remediated.
	84. Reach out to device owners through a helpdesk, and fix the security risk together with or for the device owner.
	94. Give out certificates with a date belonging to a device that state the level of security a device has at that moment, ensuring only a specified level of security is allowed and the certificate is up to date before given to new users.
	100. Give out certificates with a date belonging to a device that state the level of security a device has at that moment, ensuring only a specified level of security is allowed and the certificate is up to date before given to new users.