Are the Dutch government controls for the protection of critical telecommunications infrastructure sufficient and effective?

Erik van Garderen (s1789775)

Cyber Security Academy
Master Thesis
January 2018
Dr. Els De Busser, Assistant Professor Cyber Security Governance, Institute of Security and Global Affairs, Leiden University

Eric Luiijf MSc, Luiijf Consultancy

Abstract

This thesis is an assessment of the efficiency and effectiveness of the laws and regulation in place to govern the continuity of the critical services in the Dutch telecommunication sector. Availability of critical infrastructure in the Netherlands ranks number 5 globally. However, outages happen and have a big impact on society, especially after a prolonged time. Given the rapid change in society with regard to dependencies on communication services, the growth of equipment connected to the internet and the change in services used, it is researched whether laws and regulation help with keeping continuity of telecommunications infrastructure at the current level. An assessment of applicable laws and regulation has been made in order to understand the legal landscape. In addition, an overview has been given of telecommunication architecture to deepen understanding of continuity related issues. Based on this understanding, the systems theory has been used to model the landscape of stakeholders and the influence on each other. Using some actual cases to research the effects on society, preliminary conclusions have been drawn. These conclusions were validated by means of interviews with key employees from stakeholders. The thesis ends with conclusions and some suggestions for improvement from a legal perspective. Also some suggestions for further research have been given.

Contents

1 Introduction

The Netherlands has a wide variety of critical infrastructures, from energy distribution to water management, from payment services to telecommunications and from the police force to air transport to name but a few. These infrastructures are formally considered critical (The Dutch government uses the term vital) by the Dutch government due to the importance and value they deliver for Dutch society. The full list of critical services is maintained by the NCTV [NCT171]. This list is categorised according to the impact of society. For example, the highest category is based upon financial damage over 50 Billion Euro or over 10,000 people dead or injured. A critical service hence, is a service on which Dutch society is dependent for its well-being.

In case of outages or malfunction of these services, society can be disrupted, whereby billions of Euro of damages can occur. Some of these infrastructures are government owned or controlled whilst others are privately owned [Eer13]. In order to ensure the proper functioning of these infrastructures, laws and regulations, such as the Dutch electricity law [Dut98] and telecommunications law [Dut17] are in effect to ensure the security and continuity of these infrastructures.

A number of these infrastructures are specific to the Netherlands, such as flood defences and water management. Other infrastructures, such as high voltage electricity, financial services and telecommunications are connected to other national infrastructures and have a continental or global reach. Telecommunications services are used to provide critical connectivity and communication services to other infrastructures. These telecommunication services enable people and systems all over the world to connect to each other.

History has shown both in The Netherlands and abroad that protection of these privately-owned infrastructures can suffer due to deviating interests of the owners compared to the government. For example, the ransomware attack of mid 2017 cost Maersk over 250 Million euro in damage[Mae17]. Even though laws have been put into effect to ensure correct functioning, incidents have happened which have impacted on the availability of services as well as integrity and confidentiality of services [NOS12].

The last couple of years have shown[Kam14] that a variety of threats came to pass in The Netherlands and abroad: From hostile take-over attempts when the Mexican company America Móvil tried to take over telecommunications provider KPN [ANP13], to the IT situation in the Rotterdam region [Rek17]. From the alleged influence of Russia over the American elections [CIA17], to the report about, and the publication of, NSA and CIA technologies on WikiLeaks[Smi17]. While some of these threats did not occur in The Netherlands, there is no guarantee that these threats will not happen in the future [Hol17].

Telecommunication services are used to support every aspect of daily life in the Netherlands, for people and business and the other underlying critical infrastructures. In the event of disaster, a cascading effect is likely to occur from the telecommunication infrastructure to other critical services. The near future will bring a further reliance on telecommunications due to the development of the Internet of Everything [NCS16]. Trends in transportation and energy will also have an effect on communication[Seb17]. In every critical infrastructure sensors are used to collect information and actuators are used to control and adapt configurations. All these systems are connected via wireless and wired telecommunication networks. If, for example, locks in waterways cannot be controlled, water levels can raise and flooding can occur.

Despite the protection of Critical Infrastructures (CI) being considered a necessity by governments for the numerous centuries [Bro06], the impact of telecommunication services on such infrastructures was less clear. Almost two decades ago, the first thoughts emerged in society on the protection of critical infrastructures managed by telecommunication services. The United States was seen as the trend setter[Cli98]. In the Netherlands, in early 2000, the risk related to critical infrastructure was investigated in order to examine if extra controls would be necessary[Lui00]. In addition to these activities, supporting organisational structures such as the NCTV (National Coordinator for Terrorism and Safety) were put in

place to enhance co-operation and exchange information regarding the protection of critical infrastructure. The afore mentioned attempt by América Móvil prompted the Dutch government to propose a law to prevent hostile take-overs of critical infrastructure suppliers [Min17]. This proposal can be seen as an afterthought in the light of the privatisation of Dutch critical infrastructure. This thesis aims to assess whether the current legal controls to ensure that reliability of the Dutch privately owned critical telecommunications infrastructure can be maintained or whether extra controls are needed. The legal controls assessed can be of Dutch, European Union or other international treaty origin. The current scientific literature on the protection of critical infrastructure has a technical and organisational focus and tends to overlook the governance aspect of laws and regulations[Dun05]. In 2012 however, NATO published a comprehensive manual which takes the governance aspects into a deeper perspective and provides suggestions and best practices to improve protection of critical cyber infrastructure from a nation state perspective [Kli12].

1.1 Motivation and relevance for research

As mentioned above, telecommunication services in the Netherlands are used to enable other critical infrastructures to function. One of the earliest incidents to have nationwide impact was a telephony outage due to a popular television show in 1988. Viewers could a call a service number at the end of the show. Over a million people tried to call the number, leading to a telephony service outage[Dut061]. Another incident occurred over a decade later with an outage of the telephony systems of KPN on April 19, 2001 [AGC01]. This outage led to actions which will be discussed later in this thesis. The hack of Dutch certificate authority DigiNotar BV was a security incident in the Netherlands with worldwide impact [Pri11]. This incident was followed by the 'Lektober' awareness campaign, whereby the website http://www.webwereld.nl announced that they would publish a privacy or security leak every day for the entire month of October 2011 [Mei11]. Even though these Lektober incidents might not have had an impact on critical infrastructure, similar hacks could have had an impact on society. If attackers had abused the vulnerabilities found in the management of Dutch locks, society might well have been affected [Blo12].

Since then a multitude of events have happened both in The Netherlands and abroad whereby critical infrastructures have been impacted by hackers, from script-kiddies to state-sponsored actors [Ver17].

As discussed for the first time in The Social Contract [Rou62], a nation's government is responsible for providing safety and security to its citizens, It can be stated that governments have to ensure that society stays safe and secure controls must be in place to ensure this stability. Controls can be offered in various ways, from laws and regulations, to governmental agencies, army and police forces, etc. Governments are not only responsible for governing the infrastructure, but are also users of infrastructure itself. Even some 2000 years ago, the Roman Empire defined roads as critical infrastructure helping to protect and defend their empire. In the current era of widespread electronic communications, protection of critical telecommunication infrastructure is essential for the security and continuity of society.

Some critical infrastructures are owned by the government, however telecommunication infrastructure is not. Certain sectors of the telecommunication sector have been privatised since the early 1990s [Eer13]. This means the way the government can ensure reliable and secure telecommunication infrastructure has changed. The government is not in direct control and has to use mechanisms such as laws, regulations, legal authorities etc. The companies which own the telecommunication infrastructure are all for-profit companies. This can create a conflicts of interest between profits and reliability as mentioned in the privatisation report.

It can be questioned whether the controls available to the Dutch government are sufficient and effective in protecting the critical Dutch telecommunications infrastructure, given the importance of this sector for the security and reliability of Dutch society. (In section 4.1 definitions of effective and sufficient are given to clarify the research.) Trends such as Internet of Things (IoT), companies moving their information technology infrastructure to the cloud [Spr171], self-driving cars [CIT16] and other trends make reliance

on telecommunications even greater and hence, require effective controls to ensure the reliability of the networks.

In this thesis, the sufficiency and effectiveness of current and proposed regulation for the security of telecommunication services in the Netherlands is researched. The initial definitions of sufficient and effectiveness are based on literature research. Based on the results of the research, ideas for improvement of laws and regulation will be suggested.

The aim of this thesis is to contribute to the security and safety of the Netherlands. It is intended to help lawmakers create a comprehensive picture of the stakeholders, the complexity, options and risk related to critical infrastructure protection of telecommunications.

2 Research Questions

From a security and safety point of view, it will be investigated whether more or other controls are needed to protect the telecommunications infrastructure in the Netherlands against threats such as mentioned in the previous chapters. The main research question is:

- *Which legal controls can the government implement to gain greater control, by adapting laws and regulations, of privately owned critical telecommunications infrastructure given the threats the Dutch society is facing?*

Based on this question, some sub questions must be answered to reach the conclusion of the main research question. The government must know all the stakeholders involved and their desires, needs and drivers to use or deliver the telecommunications infrastructure:

- *Who are the main stakeholders involved?*
    - *What are their desires, needs and drivers?*

The current laws and regulations in practice must be examined for strengths and weaknesses, so a baseline for improvements can be defined:

- *What are the strengths and weaknesses of current critical telecommunication infrastructure related laws and regulations in the Netherlands?*

Within society and in the telecommunications sector numerous changes are taking place and these changes can impact the effectiveness of laws and regulations.
Dutch laws are not autonomous. The Netherlands is part of the European Union and part of the responsibility of law making falls within the European Union. Laws and regulations must fit in the European Union framework and must comply with European laws and other agreements. Standardisation of technology is an aspect which must also be taken in consideration. Networks can be connected due to standards set by institutes such as the International Telecommunications Union [ITU17], The European Telecommunications and Standardisation Institute [ETS15] and the Internet Engineering Task Force [IET17]. Telecommunications and IT companies must adhere to these standards in order to make telecommunication services possible:

- *What are the limitations and restraints which must be taken into account by new laws and regulations in the Netherlands?*

This might influence the way telecommunication service providers operate and this could have an impact on laws and regulations. In order to establish a view of what the near future could bring, the following sub question must be answered:

- *What are the expected changes and developments impacting the Dutch Telecommunications sector within the next 5 years? Which adaptations on applicable laws and regulations will be required?*

Due the speed of developments in the telecommunications sector the near future is limited to the coming five years..
Based on the previous questions, it is the intention to define areas for improvement within Dutch law and considering the needs and drivers of the various stakeholders:

- *In which ways can CII (Critical Information Infrastructure) related policies be adapted to suit future needs of Dutch society?*

3 Research methodology

3.1 Thesis setup

The research is divided in five steps, each step is split in activities and topics relevant to a specific step. These steps are specified in the following paragraphs. The setup of this thesis is shown in Figure 1. This figure shows the various chapters and paragraphs of the thesis.

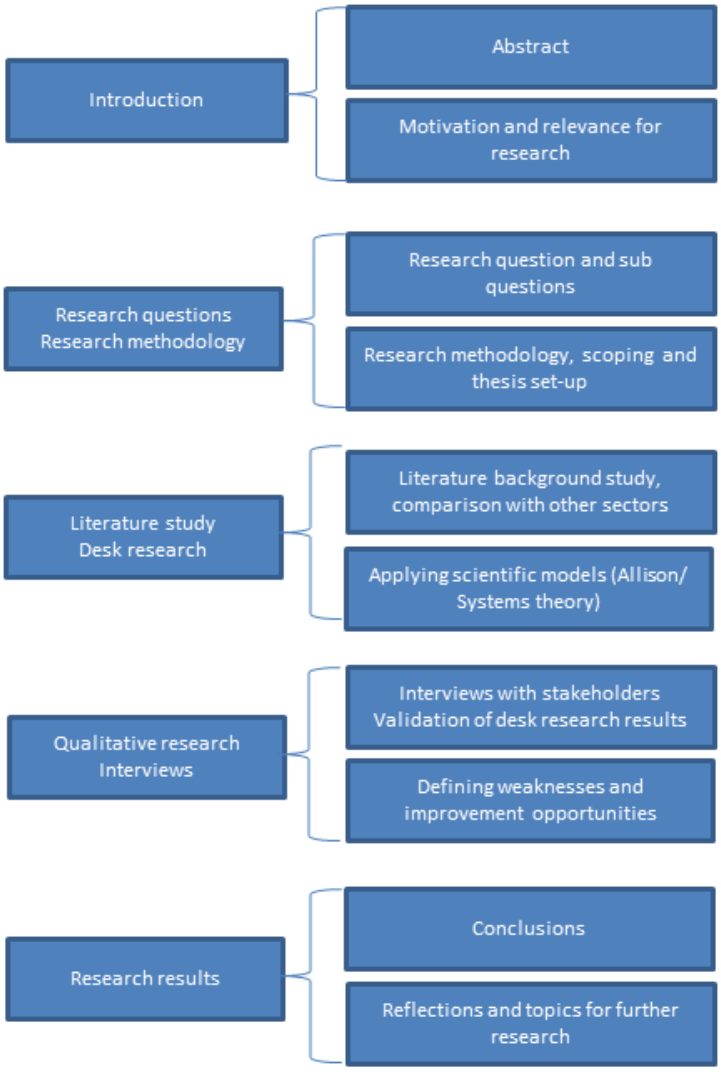

Figure 1 Thesis structure overview

Using a hermeneutical approach, by trying to reach an understanding of needs and drivers of the various stakeholders and security requirements, it is the intention to describe the effectiveness of current laws and regulations. The effectiveness is based on a combined view of all stakeholders. It has to be noted that stakeholders will not always share the same views. When viewpoints differ this will be made explicit in the research. Throughout the thesis, the research will be qualitative in nature, using literature research and interviews as the main tools to collect findings and evidence. From a social science perspective, the research will be analytically descriptive in nature. In order to gain a better understanding of the

interactions between the various stakeholders and law makers, the systems theory has been used to model the landscape of stakeholders and their interactions.

The second part will introduce the research questions and sub questions, which will be answered in the thesis. The questions are elaborated upon in chapter 2 of this proposal.

The research methodologies to be used will also be discussed and motivated in this part. The research will contain a part consisting of desk research and a validating section in which interviews with stakeholders are used to establish a clear view of whether the current laws and regulations need to be adapted to ensure a good fit to future needs. This view will be based upon stakeholder motivation, intentions and expected future expectations.

Using a social sciences perspective, the systems theory is used to model the various stakeholders in order to organise the risk and benefits of the existing and proposed laws.

The research will start by describing the setup of the critical telecommunication infrastructure in The Netherlands. Also an inventory of stakeholders will be made. Next to the identification of stakeholders, an inventory of applicable law and regulations will be made. The scope and effectiveness (in theory and practice) of the law will be analysed.

Due to the fact that effectiveness of laws and regulations can be interpreted in different ways, the various stakeholders will also be asked what their expectations are with regard to these laws and regulations. Their answers will be added and merged with the definitions, in order to gain a common understanding and obtain reproducible results.

Based on the stakeholder and legal analysis, a model will be defined which will show how the laws affect the various stakeholders and what might be missing to ensure security and availability of the infrastructure.

In the next phase of the research, the model and defined criteria will be used as a baseline for interviews and surveys with representatives from the various stakeholders. From a research perspective there is a preference to hold interviews with stakeholders. For stakeholders such as consumers, interviews will be difficult to undertake given the fact that there are many types of consumers. Surveys are expected to give better results.

Based on the interviews and surveys, the model will be assessed based on the criteria defined and adapted to include the insights and findings of the interviews and survey. This model will then be finalised. Areas of legal improvement to obtain more control will be proposed from both a Dutch and a European perspective.

The thesis will end with the conclusions of the research. It reflects on the research and offers suggestions for further research.

3.2 Scoping and methodology

Given the proposal of the Dutch government to devise new laws to secure Dutch critical infrastructure, the scope of this research will be limited to the Dutch privately owned critical infrastructure and the laws and regulations used by the Dutch government to keep critical infrastructure in the Netherlands safe and secure. Other countries have expressed concern about critical infrastructure. For example, in the United States there are concerns that the Citgo assets could fall into Russian hands due to a Venezuelan company default [Sir17], Such cases will not be taken into consideration in this research unless it is deemed relevant in relation to Dutch critical infrastructure. Due to the fact that the Dutch government also has to comply to European Union laws and directives, these will be taken into account as well. Threats will be considered on a high and generic level and in relation to the laws and regulations which are meant to protect against these threats.

The critical infrastructure landscape contains a wide variety of different infrastructures. The Dutch Coordinator for Security and Counterterrorism (NCTV) maintains the list of services deemed critical for the well-being of Dutch society [Nat16]. Entities are placed on this list based on criteria with regard to financial damage and the number of citizens potentially wounded or killed due to a crisis caused by a critical infrastructure service.

The scope of this thesis is limited to the telecommunication infrastructure mentioned in the NCTV list. The fact that these critical infrastructures are privately-owned has an impact on how laws and regulations should be designed. Due to the fact that telecommunication infrastructures are used to support almost all other critical infrastructures, the scope of this thesis will be further limited to the basic connectivity services in the mobile and fixed networks, including the necessary services to ensure reachability of services (addressing and number portability services) and secure communication (certificate services).

Only The Netherlands itself is examined in this thesis. The overseas countries and municipalities of the kingdom are not taken into account. The situation is not comparable to the Dutch situation as shown in a report showcasing the issues and recommendations[Bui16].

As Myriam Dunn [Dun05] describes in her paper the socio-political dimensions of critical information protection. There is a need for a social science approach to research developments and issues in the protection of critical infrastructure. In her paper she describes three protection typologies for critical Information Infrastructure protection (CIIP):

- *CIIP is an issue of national security*
- *CIIP is an issue of economics*
- *CIIP is an issue of law enforcement*

The third typology is out of scope for the research in this paper. It is not considered relevant for the protection of the critical telecommunication infrastructure in itself, but purely as one of the telecommunications services which must be protected. The other two typologies were described in Jeroen Veen's thesis regarding the position of Dutch government towards encryption [Vee17]. In his thesis Veen uses the governmental decision-making models as defined by Allison in his papers about the Cuban missile crisis [All]. Veen calls these typologies 'lenses' and also used a 'privacy lens', which is out of scope for this thesis. As the Author, I consider the General Data Protection Regulation [Eur16] sufficient enough to omit the privacy lens in this thesis and focus on the national security and economic lenses.

In order to understand the sociological impact of the laws and regulations on the protection of telecommunication infrastructure, the laws concerned will be analysed to identify primary stakeholders, which stakeholders are protected, which stakeholders must implement controls and what the effects are of these controls to ensure reliability. Primary sources in this phase of research are the laws and regulation text which are accessible from websites of the European and Dutch governments. In order to determine effectivity and consequences of the laws and regulations, stakeholders will be interviewed. Due to the expanse of the telecommunications market, only a limited number of people can be interviewed. The focus will be on governmental stakeholders, telecommunication provider stakeholders and a selection of other stakeholders. The opinions and experiences of the stakeholders, in combination with the findings of the desk research will be used to assess the effectiveness of laws and regulations. Due to the fact that I work for one of the Dutch telecommunications companies, the thesis also elaborates on the dangers of writers' bias.

4 Literature study and desk research

This chapter discusses the current situation with regard to the critical telecommunications infrastructure. In order to understand the laws and regulations surrounding telecommunication, it is important to realize how telecommunication networks are built and how these networks are interconnected and managed. The following chapters deal with each of these aspects.

4.1 Definitions

One word in the title of this thesis is paramount. The word 'sufficient'. What are sufficient controls with regard to governance of the telecommunications critical infrastructure? According to Merriam-Webster, the definition of 'sufficient' is "*enough to meet the needs of a situation or a proposed end*" [Mer17]. This definition is not an accurate definition: What is enough and what are the needs with regard to the protection of Dutch critical telecommunications infrastructure? Both literature research and interviews will be used to establish a common definition of this term.

Laws should not only be sufficient, but also effective. Effective is described by Merriam-Webster as "*producing a decided, decisive, or desired effect: an effective policy" [Mer171]*. Here it can be questioned what the desired effect will be. It depends on the perspective of the stakeholders, what they will see as a desired effect. In this thesis, the perspective of the government is seen as leading due to the government needing to be in control of continuity of critical infrastructure [NCT171].

There being multiple stakeholders involved, the definitions of sufficient en effective will be verified with the stakeholders in an attempt to reach a consensus and definitive meaning.

In this thesis, laws are defined as the set of rules established and based on articles 82-88 of the Dutch constitution [Dut08]. These rules regulate all participants in society and important aspects of society. Laws, regulations and the consequences for not abiding by these are in place to organise society. The definition of regulation in the Oxford Dictionary is "A rule or directive made and maintained by an authority" [Oxf17]. For the sake of this thesis, regulation is seen as a set of rules which govern certain aspects of society without being formalized as a law. Regulations can be statements issued by governmental organization emphasising a government's point-of-view. For example, governmental institutes such as ACM (Authority for Consumers and Markets) have issued statements on how private parties have to act in situations with limited competition. An 'Algemene Maatregel van Bestuur (AMvB, or general governmental regulation) is also seen as regulation. An AMvB can be related to a law or be used stand-alone. Some laws refer to AMvBs to detail certain aspects of implementation. AMvBs are easier to adapt and change than laws can be adapted or changed.

With regard to the protection of critical infrastructure, three definitions are often used: Confidentiality, Integrity and Availability. Within this thesis, the definitions are those of the international standard ISO-27000 [ISO16]. These definitions are defined as:

- Confidentiality: "*property that information is not made available or disclosed to unauthorized individuals, entities, or processes*"
- Integrity: "*property of accuracy and completeness*"
- Availability: "*property of being accessible and usable upon demand by an authorized entity*"

4.2 Laws and regulations

This chapter describes the current laws and regulations in effect with regard to robustness and reliability of telecommunications. Telecommunication laws from other viewpoints such as competition, mobile frequency usage, lawful interception, etc. are not taken into account as these are out of scope for this research. A comprehensive overview of Telecommunication law in the Netherlands can be found in the book by Knol and Zwenne [Kno15]. This chapter describes the characteristics of applicable law with regard to continuity of critical telecommunications infrastructure.

Dutch laws cannot be seen in isolation. Articles 93 and 94 of the Dutch constitution [Dut08] describe the relationship of Dutch law within international treaties and agreements. The most important international treaty for Telecommunication is the Treaty of the European Union [Eur162]. This treaty was ratified by the Dutch government in 2008 [Dut081]. This treaty stresses the importance of infrastructure in 'Title XVI, Trans European Networks' and gives the baseline for other EU directives, and regulations. Regulations can

be seen as laws and are in effect immediately after signing. Directives require national governments to set up laws and regulation before the date set in that specific regulation.

The following paragraphs contain the laws and regulations in effect for the protection of critical telecommunication services.

4.2.1 International treaties and co-operation

For this thesis some international treaties and documents are of importance with regard to critical infrastructures.

- In 2001, the Council of Europe established the convention on Cybercrime [Cou01]. This is an international treaty with the objective to reduce cybercrime by enabling international co-operation. The treaty was ratified by the member states of the Council of Europe, and by other nation states such as the United States of America, Canada, Israel, Japan, Panama and others. This treaty is important as it allows law enforcement agencies to co-operate in combating international cybercrime.
- The NATO Co-operative Cyber Defence Centre of Excellence published a manual with recommendations and good practices for the improvement of reliability and cyber security of nation states. This manual not only addresses technical aspects, but also has chapters devoted to governmental aspects of reliability and continuity of cybersecurity [Kli12].
- In 2013, at a NATO cyber conference in Tallinn, a manual on cyberwar was published [Sch13]. This manual gives guidance to the application of international law on cyberwarfare operations. The manual also states actions against a nation states critical infrastructure and hence, can have impact on Dutch critical infrastructure during a time of war or aggression. Article 61 of this manual addresses the topic of using ruses. Based on the recent 'Fake news' discussions in the media, further research is suggested to see how this kind of attacks can be minimised[AIV17].

From an international point of view, there are councils and conventions which help to shape part of the legal framework for security and continuity. These forums do not provide laws and regulations, but it can be expected that laws and regulations will use best practices to improve security and availability of infrastructure.

- FIRST is the International Forum of Incident Response and Security Teams. This forum helps its members in finding each other to fight cybercrime incidents and help each other with best practices and recommendations. The member list of FIRST shows that critical telecommunication providers, some banks and the government have CSIRT or CERT capabilities, but other sectors of the critical infrastructure are not present[FIR171].
- In 2015 the Global Forum on Cyber Expertise was founded in The Netherlands. 38 nation states, international organisations and a variety of suppliers participate in this forum[Glo15]. This forum aims to improve reliability and security by structural development of best practices.

The European Union has also established institutes such as ENISA [ENI17] and ETSI [ETS15] to help in standardizing protocols, procedures and ways of working within the Telecommunication and IT sector. Even though these institutes are not law making and regulation agencies, their council and standards help to increase resilience, robustness and interworking.

ENISA is the European Union Agency for Network and Information Security[ENI17]. This agency acts as the European Cyber Security Incident Response Team (CSIRT) and advises the European Union on cyber issues. It also assists other CSIRTs (or CERTs, Computer Emergency Response Team) with solving cybersecurity incidents. Every country and most larger companies have their own CSIRT or CERT and these teams co-operate to fight cyberattacks. ENISA has a liaison with FIRST [FIR17].

4.2.2 European laws and regulations

In contrast to my definition in section 4.1, The European Union uses a different definition of regulation. A regulation according to the European Union is a European law which does not need transposition to national law, while a directive sets minimum goals and member states must transpose directives into national law [Fre05]. In this section, the EU definition is used.

- The European Union has a framework directive (2002/21/EC) for regulation of electronic communications service providers [Eur02]. This framework addresses the functioning of national authorities with regard to Telecommunication and includes articles on integrity and security of public networks, including privacy of citizens.
- From a reliability point of view, the EU directive on Network and Information Security (NIS, 2016/1148) is the most important regulation available. [Eur161]. The first proposals were made in 2013 and the directive became effective in 2016. This directive must be implemented within national law by all EU member states before May 10th , 2018. Companies which must adhere to the law must be assigned before November 2018. This directive addresses the risk of cyber incidents as a result of attacks, technical failure or viruses. It has three objectives:
    - Member states must create a minimum level of national capabilities.
    - National competent authorities must be able to co-operate.
    - A culture of risk management and information sharing must be created.
- The scope of the NIS-directive is not limited to the telecommunication sector, but includes sectors such, but not limited to, as transport, energy, banking, healthcare and drinking water. Internet exchanges, name and certificate service providers, and other parties delivering critical infrastructure services are also in scope for this directive. National governments must assign the Operators of Essential Services which must be included under the NIS before November 2018. An important provision in the NIS is the requirement for companies to notify a competent national authority when security incidents are detected. The reasoning is that public awareness can be raised, incidents can be solved faster and with less impact when companies are assisted with troubleshooting and problem solving. The NIS even provides for international co-operation, when the needs arises.
- The EU also has set guidelines for the improvement of Telecommunications infrastructure in regulation 283/2014 [Eur14]. This regulation has the objective of improving security and the reliability of networks by enabling funding for research on improvement of the telecommunications infrastructure. This guideline also promotes cross-border co-operation with regard to security of digital infrastructures.
- The EU regulation on the generic data protection (GDRP) which comes in effect on May 25th , 2018 is also a means of helping to protect critical infrastructure [Eur16]. Even though this regulation is meant to protect the privacy of European citizens, every company handling privacy sensitive data (including telecommunications companies) needs to incorporate extra controls to ensure compliancy to this regulation. These added controls will also improve the security of the telecommunications network as privacy enhancing controls also improve security.
- The European Union is also rewriting the laws with regard to Electronic Communications (EECC) [Eur163]. As part of this proposal OTT (Over-The-Top) players are taken into consideration with regard to this new law, as are new developments such as Internet-of-Things, Cloud computing, eHealth, autonomous vehicles and a wide variety of other new developments. The EECC is an improvement and rewrites an older law, previously revised in 2009. The European Union is rewriting this law due to the higher impact of critical telecommunications infrastructure on society and the importance as seen by the European Union for the development of the Digital Single Market (DSM). High capacity and high availability connectivity are seen as major objectives by the proposal. Some of the means in the directive include national competent authorities and regulatory offices, including procedures to harmonise the regulatory framework in Europe.
- For electronic identification and business, the EU has established the so called eIDAS regulation 910/2014 on electronic identification and trust services [Eur141]. This regulation has articles devoted to the security of these services. This regulation has been binding since its publication on 23rd of July

2014. The relationship to telecommunication services is a minor one, however because of consumers using mobile phones to prove identities, telecommunication service providers have to adhere to the requirements as set out in this regulation.

4.2.3 Dutch laws and regulations

The European Regulations are binding as soon as they are signed. Directives will need a transposition into national law. There are also Dutch laws to safeguard Telecommunications and critical infrastructure. The following laws and regulation have been found to be of importance to the continuity of Dutch telecommunication infrastructure:

- The Dutch constitution [Dut08] has article 13 dedicated to the confidentiality of communications, including electronic communications. The constitution is the foundation of all other laws and regulations in The Netherlands.
- The Telecommunication law [Dut17], is the most important control tool for the management of telecommunication infrastructure in the Netherlands. This law has been aligned with European regulation in order to harmonise laws with other EU member states. Chapter 11 of this law handles all issues related to privacy and business continuity, while chapter 14 gives directions during emergencies.
- The Telecommunications law also has been adapted to include services of identity providers, based on the law on electronic signatures [Dut03]. This law includes continuity and security requirements.
- In addition to the Telecommunications law, additional laws have been written to describe how specific continuity topics must be implemented in a governmental decree [Bes12]. Specifically for the critical infrastructure providers of the telecommunication sector, there are additional regulations for continuity management in relation to citizens, technology and processes [Dut14] within telecommunication service providers which own and operate a major part of Dutch telecom infrastructure. Quantifiable controls which state minimum requirements for uptime etc. are not mentioned in this law or in any other regulation.
- The emergencies referred to are further addressed in the Dutch law for extraordinary circumstances and emergencies [Duc16]. This law addresses emergency situations and details how crisis management situations must be managed from a government perspective.
- A specific law requiring companies to keep information secure is the Dutch privacy law (Wet Bescherming Persoonsgegevens) [Dut00] based on the previous European privacy regulation. This law will be replaced by the General Data Protection Regulation (GDPR) regulation on May 25th , 2018[Eur16]. This GDPR sets strict requirements for companies with regard to handling of privacy sensitive data. In case of non-compliance, fines up to 10M Euro or two percent of the annual turnover of the previous year, can be issued. Should malicious intent be proven, these fines can be doubled. This will be a driver for companies to improve security and hence benefit security and continuity of telecommunications infrastructure.
- The law on the Security Regions (Veiligheidsregio's) sets requirements for telecommunication services and the continuity of communication services in these regions[Duh17]. The national law on extraordinary circumstances prevails over this law in situations covering more regions or during extraordinary circumstances. This law is relevant for critical telecommunication providers as the various regions must carry out controlled real life trails and telecommunications service providers must take part in based upon article 14 of the Telecommunication law.
- The law on government claims (Vorderingswet) grants the various ministers the right to claim ownership or usage rights of private property in case of specific circumstances (Dutch Government, 1962). This law is cited as it possibly played a role in the, DigiNotar case [Don11]. The articles in this law allow the government to act in crisis situations.
- The Dutch law on military affairs contains various articles which give the Military control over telecommunications infrastructure in cases of emergence [Dut99]. These articles have never been used.

The Dutch ministry of Defence is working to update cyber capabilities [Def17]. Consequences for this law on the critical telecommunication infrastructure and cyber capabilities are unknown.

- The laws on computer criminality (Wet Computercriminaliteit II [Dut991] and Wet Computercriminaliteit III, which is not yet in force[1]) have been researched to examine the relationship between the availability and integrity of critical infrastructure. The objective of these laws is to improve law enforcement and cybercrime and thus decrease economic damage to society. These laws do not specifically mention continuity of services, but the content helps to fight cybercrime. Hence availability can be improved by deterrence.
- The law on security clearances has requirements for employees working on critical infrastructures [Dut96]. In addition, the Dutch AIVD security agency has published guidelines for commercial organisations to establish a baseline of functions within those companies which need a security clearance [AIV14]. Certain aspects of operations may only be performed by employees with a security clearance.
- In 2001, immediately after the auction of mobile frequencies, the five operators asked the former authorities NMA, Opta[2] and the ministry of economic affairs whether co-operation was allowed in the roll-out and exploitation of the network. Lower consumer prices and better coverage were cited as the reasons behind this proposal. The government responded with some very strict guidelines, but declined the request to work together as such. Only site sharing was allowed[NMA01]. Besides laws in effect to protect critical infrastructures, there are also laws which define organisations and councils. These organisations provide counsel and advice to the various governmental departments and to House of Representatives and Senate. When these organisations have an impact on critical telecommunication infrastructure, these are mentioned.
- The National Cyber Security Centre is the governmental organisation responsible for increasing resilience against cyber threats in the Netherlands. NCSC is a subsidiary of the NCTV (National Coordinator Terrorism and Security) department, which is part of the department of Justice and Security. The NCSC monitors for threats and incidents, ensuring crisis are handled in an effective way. NCSC also helps to increase co-operation in private-public-partnership settings [Nat171]. The NCSC organisation also reports current cyber threats, to help government and private institutions with cyber risk assessments [NCS16]. These annual strategic risk assessments are part of a national security plan comprising both NCTV and NCSC input. In the future the assessments will be made every four years. The granularity increase is seen as a big step, however, the documentation does not give motivations and drivers for this change [Ste16].
- In 2014, a council for the environment and infrastructure (RLI, Raad voor de leefomgeving en infrastructuur) was setup [Dut142]. This council advises the government on issues regarding infrastructures and environment, including the continuity risks.
- Another council which has been setup is the Cyber Security Council (Cyber Security Raad). This council advises the Dutch government on cyber security risk related to the Dutch IT infrastructure. The Cyber Security Council is setup with members in top governmental positions, private companies and educational institutes [Cyb17]. The council advises on numerous subjects, such as current IT related issues, assistance in crisis management and advice on the implementation of the National Cyber Security Strategy. The Cyber Security council was actually been created as a result of the first National Cyber Security Strategy [Nat17]. This strategy was written to assist the government in setting

1 The Senate website contains information about the current state of affairs (https://www.eerstekamer.nl/wetsvoorstel/34372_computercriminaliteit_iii)

2 NMA is the former national authority for consumer and market, OPTA is the former authority for telecommunications and mail services. These organisations are merged into a new authority, called ACM per January 2013. The consumer authority (CA) was also part of this merger[ACM17].

goals and priorities to increase resilience against cyber threats. The current version of this strategy [NCT14] has five goals:

1. Increase resilience against cyber-attacks
2. Reduce cyber criminality
3. Invest in security and privacy protecting services and products
4. Co-operate with other countries and institutes to increase security, safety and peace within the cyber domain.
5. Invest in well educated people to ensure innovation can keep up with cyber security requirements.

4.3 Who are the main stakeholders?

This chapter deals with the identification of stakeholders within the telecommunications sector and their interactions. The research of applicable laws and regulations was used as the main indicator for determine the stakeholders concerned. Given the number of individual stakeholders, only the stakeholders relevant to my research have been elaborated upon. For each of the stakeholders, a short overview is given based on security and economic perspectives or lenses. The security and economic lenses as applied by Veen in his thesis of the emergence of the Dutch view on encryption encourage looking at the effectiveness from these two angles [Vee17]. The systems theory, defined by Bertalanffy, was used to model the system and the major partakers. [Ber68].

4.3.1 European Government

From a law and regulation perspective, an important part of regulation is developed by the European Union government. The Dutch government is one of the member states and has to ensure that directives are enforced and laws are passed within the time lines set by the European union. The European continuously strives to improve security, safety and prosperity within all member states [Eur12]. Nation state governments have transferred part of their sovereignty to the European Union. This transfer of sovereignty aids the development of harmonised laws. Having the same law in every member state (harmonisation) helps with economic development. The process of law making is complex and lawmakers need knowledge of the sector for which laws are made for. Within a legal framework, all aspects of society must be taken into consideration. These include security and economy, safety, privacy and how the law will affect people and institutions. Consultation is a standard means of obtaining opinions and knowledge of the stakeholders. These consultations are input for the final laws and regulation. The entire process is referred to in the EU guide to the EU institutions of 2012.

4.3.2 Dutch government

The Dutch government (and it's alliance of European lawmakers) is one of the most obvious stakeholders with a wide variety of roles. The government acts as lawmaker, auditor, consumer of infrastructure for general purposes, and takes on roles within diplomatic communications, military connections and lawful interception. In the research, these roles must be reflected upon when considering governments interests and principles.

The past three decades have seen changes in the governance of critical infrastructures and other government owned assets. The privatisation of these assets has been undertaken in a variety of ways [Eer13]. The report by the Dutch government institute focuses on the why and how the various government controlled organisations were privatised and how the government could maintain an auditing and controlling role, given the fact that these privatised organisations were providing important services to Dutch society. It is therefore imperative to provide a comprehensive insight into how the government dealt with the privatisation of critical infrastructure.

The Dutch government is organised into various departments[Rij171]. Within the Telecommunication sector, the department of Economic Affairs and Climate Policy (EZK, Ministerie van Economische Zaken & Klimaat) is important due to the fact that anti-trust and continuity aspects of telecommunications are regulated by this department. The department of Justice & Security (Ministerie van Justitie & Veiligheid) is

responsible for regulation of lawful interception, cyber security and the 112 emergency number. The Ministry of Interior and Kingdom Relations (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, BZK) is an example of the government as a consumer. The BZK department is responsible for the internal government telephony communication service called OT2000 [AGC98].

4.3.2.1 Crisis management

The J&V department is responsible for crisis management[3] in the Netherlands [NCT16]. In the Crisis management handbook, all principles and guidelines for crisis response are discussed. Should a crisis occur, an Interdepartmental Commission Crisis Management (ICCb, Interdepartementale Commissie Crisisbeheersing) can be setup to normalise a crisis situation. The National Coordinator for Terrorism and Security (NCTV, Nationaal Coördinator Terrorismebestrijding en Veiligheid) would usually chair ICCb. In certain cases, the minister of General Affairs could act as chairman. Should a crisis arise whereby national security could be impacted, an Ministerial Commission Crisis Management (MCCb, Ministeriële Commissie Crisisbeheersing), could be setup to deal with political issues of a crisis. The minister for J&V would be the chairman unless the minister of General Affairs decides that he should take charge. When in effect, these bodies are situated at the National Crisis Centre (NCC).

The National Cyber Security Centre (NCSC) must be notified when a Cyber security related incident occurs. This obligation is a consequence of the implementation of the European Union Network and Information Security directive (NIS). The NCSC acts as the regulatory oversight organisation for the NIS. The NCSC can help the organisations which have reported an incident in various ways depending on the incident or crisis. The NCSC is a sub-department of the NCTV department. During cyber incidents, the NCSC can activate the ICT Response Board (IRB). The purpose of this board is to advise the ICCb during the crisis. Members of this board are employees of private partners and of government departments and can be requested to assist depending on the specific aspects of a crisis. [NCS17]. The NCSC is not only involved in crisis management, but also deals with prevention, information and knowledge distribution. An exact list of NCSC services is available in a service catalogue [NCS171].

There are other departmental structures and organisations within EZK fulfilling roles in crisis management. These departments are not relevant for the background of this thesis (although their role is relevant in crisis situations).

4.3.2.2 Governance

Governance aspects of the telecommunication sector are mostly handled by EZK. There are multiple governance agencies within EZK. Anti-trust and competition perspectives are handled by the ACM (Authority for Consumers & Markets). Telecommunication providers which provide public telecommunications services have to be registered with the ACM [ACM171]. Regulatory oversight is provided by ACM with regard to anti-trust aspects and by the AT Telecommunication Office (Agentschap Telecom) for continuity and security aspects of the telecommunication provider operations, including 112 and legal interception. AT publishes an annual report with relevant details of their regulatory oversight[Age17].

The Dutch Data Protection Authority (AP, Autoriteit Persoonsgegevens) is responsible for regulatory privacy oversight. The AP is an independent organisation with a report lines to the V&J department. As privacy related aspects are out of scope for this thesis, the AP is not further elaborated upon. Within EZK, the sub department for Telecommunication, Energy and Anti-trust (Directoraat Generaal, Telecom, Energie en Mededinging) handles communication with telecommunication service providers. This sub department organises the National Continuity Board for Telecom (Nationaal Continuïteitsoverleg Telecom).

The NCO-T was established in 2007 and is the successor to NaCoTel (National Continuity Plan Telecommunications)[Hee07]. NaCoTel was the public-private-partnership setup after the telephone

3

system outage of 2001[AGC01]. The NCO-T members are EZK, AT and the critical telecommunication providers. The primary goal of the NCO-T is to fulfil the obligations of chapter 14 of the telecommunication law by preparing for incidents. The second goal is to improve robustness of critical telecommunications infrastructure by encouraging parties to work together (if competition constraints allow) and by knowing how to reach and where possible help each other during continuity issues (e.g. regional roaming). The topics discussed within the NCO-T also help EZK to form regulation and inform the responsible minister about issues in the field of critical telecommunication infrastructure. The EZK department manages the NCO-T handbook [EZD06] and it's extensive appendices [EZD08].

4.3.3 Standardisation institutes

Connecting world wide networks requires standardisation. Within the telecommunications sector, the International Telecommunication Union is one of the oldest institutions[ITU17]. The ITU is a United Nations organisation, with countries, academic institutions, telecommunication sector service providers and suppliers as members. The ITU standards facilitated the worldwide telephone and fixed line communications along with numerous related aspects such as availability, security, billing to name but a few.

In the European Union, the ETSI (European Telecommunication and Standardisation Institute) the European Standards Organisation (ESO) for telecommunication infrastructure was established in 1998 [ETS15]. The ETSI establishes consensus based standards for interworking, based on input from member organisations (National standards organisations, such as the Dutch NEN), politics and companies working in the telecommunications sector.

The International Organization for Standardization (ISO) is an independent institute, with 162 national standards bodies as members[Int17]. ISO has a wide range of standards on all kinds of topics, including Information Security and Business Continuity Management.

The Internet Engineering Taskforce (IETF) is another standards organisation[IET17]. This organisation was established within the academic domain, no membership needed. Any individual can help to create and improve standards. These standards are consensus based, using humming as a voting mechanism. This is done to help the member states with less democratic values. [Res14].

Other specialised standard bodies include the American NIST and ANSI and mobile network specific standard bodies such as GSMA, 3GPP, LoRa Alliance. Information Technology specific standards bodies include the Cloud Computing Association and Cloud Security Association. A generic overview of these bodies can be found on Wikipedia [Wik171].

All these standard bodies produce standards which improve interworking, but there is a risk that standards will not conform to laws and regulations. According to ETSI, their standards are in line with EU laws and regulations[ETS15]. The IETF humming procedure indicates that care must be taken before standards can be approved. Influencing standards has previously happened and will probably happen again. An example is the weakening of American encryption standards by an American spy agency [Gre13].

4.3.4 Telecommunication service providers

The telecommunication service provider industry is seen as the other important stakeholder. The traditional service providers are the actual owners of the infrastructure and are the entities providing services to individuals, business and governmental organisations. It has to be noted that certain telecommunication service providers do not own their network, but hire capacity from other telecommunications service providers.

Service providers operating in a competitive market choose a market strategy to attract customers. They may focus on reliability, low-budget, features and other aspects of marketing, and not necessarily choose for continuity.

The bigger telecommunication companies in the Netherlands, Vodafone/Ziggo, T-Mobile and KPN own fixed and mobile networks. In the telecommunication sector there are also operators using the infrastructure of other operators, so called Mobile Virtual Network Operator (MVNO). These companies have a contract with one or more providers to share parts of the providers networks. These MVNOs make availability and quality agreements with the providers they use. The Dutch government has set rules for obligatory sharing of copper and fibre-optic networks by KPN as part of the controls to reduce the monopoly position of KPN. All relevant laws and regulation with regard to continuity are also applicable for this part of the KPN services.

In the sector, mergers and acquisitions can take place, but anti-trust laws are used to ensure that there are enough players (and networks) in this sector [Vro17]. Certain providers have also outsourced part of their operations to so-called Managed Service Providers (MSPs) [ANP12]. These MSPs manage the daily operations of the networks for the providers, but have no involvement in the business. These companies have ample knowledge of the networks they manage, but are not players when it comes to continuity and security of the telecommunication services.

Next to the traditional stakeholders, there are other providers and companies delivering infrastructure services. A prime example is the AMS-IX, which is the world's biggest internet exchange [AMS16]. Internet exchanges connect internetworks and other exchanges, thereby shaping the world-wide internet. In the Netherlands, there are some ten internet exchanges, of which two are in the world top-ten with regard to throughput and number of connected networks [Dat17].

Organisations providing name-services, registries and/or certificate services are also important stakeholders. These parties provide trust and manage the 'phone books' of the various networks. For telephony, the COIN foundation [Sti17] manages which operator uses which telephone number. Organisations such as SIDN (Stichting Internet Domeinregistratie Nederland) perform a similar role for Internet based communication[SID17].

Companies providing housing and hosting services for computer services (e.g. cloud-services) are another type of player in the telecommunication sector. Even though they do not deliver public services, these companies can deliver services to larger institutions and hence have an impact on society.

Currently, these providers are not regulated by the Telecommunication law, but failure of their services can have an impact on Dutch society. The NIS directive is applicable to these companies, when they provide essential services to society. The government must create and maintain a list with companies which have to adhere to the NIS. These companies are called Operators of Essential Services (in Dutch Aanbieders Essentiële Diensten) Given the wide range of companies and services provided, this is a major task, whereby European Union aims for co-operation between member states in order to define the companies which are considered essential for the telecommunication sector.

4.3.5 Customers of telecommunication infrastructure

Organisations and individuals using the critical infrastructure are the third major stakeholder. These stakeholders benefit from using the telecommunications infrastructure for leisure and business purposes and appreciate an available and secure infrastructure. Both commercial organisations and individuals have high expectations when it comes to the quality and availability of the services used. It must be noted that the Dutch government is also a customer of telecommunication services.

Within the telecommunication sector, it is hard to define a service for which there is no competitor providing a similar service. The pager network (Semafonie) is an example of a service without competition in the traditional sense. Competition gives customers a choice and encourages providers to be innovative and alert. Even though continuity is considered a commodity factor in communications, a provider which experiences problems with delivering continuity will lose trust and eventually customers.

Certain groups of customers have organised themselves to strengthen their relationship with providers. There are interest groups of corporate institutions with special interest in communications (BTG), the

Confederation of Netherlands Industry and Employers (VNO-NCW) which has a more generic nature. Shareholders have their interest groups which participate in society regarding topics in the telecommunications sector.[htt17]. For consumers, there is the consumer's protection foundation (Consumentenbond).

Private consumers and small business are the biggest group of customers in numbers of mobile and fixed connections. In the future the amount of IoT (Internet of Things) connections will be higher that the number of people connected [Meu17].

4.3.6 Other major stakeholders

During the research other stakeholders have been defined of which two need special attention.

Telecommunication services are dependant on electricity providers. Without electricity, telecommunications providers cannot deliver their services. The electricity sector on the other hand, depends on telecommunications to solve outages fast and effectively. Electricity engineers need mobile communications to ensure that they can work effectively. This circular dependency is also a subject for concern, as will be explained later in this thesis.

The other major stakeholders are the over-the-top players. Companies are called over-the-top, if services are delivered on top of regular connectivity services, without using the communication services provided by the traditional telecommunication service providers. The companies, such as WhatsApp, Facebook, Twitter, etc. are mostly American corporations providing worldwide social media services. Their customers are companies paying for their services to get a better insight in their marketing. Their users are citizens of countries worldwide and the user base can be in the billions. Over 2 billion users for Facebook, 1,3 billion users for WhatsApp, Twitter is 'relatively small' with only 328 million users [Sta17]. Governments are also active users of these services. Evidence could not be found as to whether governments are also paying consumers of these services. In other words, if governments pay to acquire detailed insights in the actual data collected by these OTT players. From a crisis management perspective, it is expected that law enforcement and crisis organisations use the freely available trending topic tools provided by the OTT players, although this has not been verified for this thesis.

4.4 Which telecommunication/ICT services are critical

The Dutch government has designated critical processes which those critical to the Dutch society and hence, those related to telecommunications are in scope of this research. The ICT/Telecom sector is one of the sectors. The government has assigned the services in these sectors as 'category B' [NCT17].The services included are Internet- and data services, internet-access and data traffic, 112, voice and SMS services. All these services must support mobile and fixed connectivity [Ste16].

The list of critical services details specific services such as pager services and the Nood Communicatie Voorziening (NCV, or Emergency Communication Facilities). This service is a separate communication network, in case of national outages of regular voice communication systems [Kro13]. OT2000 is not mentioned , although this network is used for communication within the various (crisis management) departments of the government. The NAFIN network is not mentioned either. This is the network of the Dutch Armed Forces, which is also used to provide part of the connectivity of the C2000 network [Gel16]. C2000 is the default mobile nationwide communication system for emergency services and government [C2018]. These services are implicitly mentioned as part of Public Governance.

A new service which is ordered by the European Union is the e-Call emergency service which must be built into new cars from April 2018 onwards. In case of a car crash, this service will automatically call the European 112 service and forward details such as activation of airbags and location of the vehicle determined by Galileo satellite. [Eur15]. This service relies on the critical 112 service for an optimal functionality.

From a European perspective, the Network and Information Security Directive (NIS) specifies essential services and has law and regulation for these services in place. DNS, name registries, digital certificate providers and Internet Service Providers are viewed as essential. [Eur161]The NIS does not distinguish between fixed and mobile communications as both are considered equally important. Operators providing such services will face laws and regulations which have to be in place May 9th 2018. The Dutch government must name the operators delivering such services (Operators of Essential Services) by November 2018.

It is surprising to discover that apart from Internet connectivity services, nothing is specified about the over-the-top services. Even though SMS services are still widely used for two-factor authentication of a variety of services, SMS services have been replaced inadvertently by consumers by other form of communication provided by over-the-top players.

One of the most visible uses of an over-the-top (OTT) service is the use of WhatsApp for neighbourhood-watch groups. These groups use WhatsApp as the primary communication channel to report safety and security irregularities in a neighbourhood. There are already over 7500 of these neighbourhood watch groups in The Netherlands and Belgium [WAB17].

The trend in using cloud based services makes cloud providers an important part of telecommunication infrastructure. Cloud services can be delivered from all over the world. Big players in this field are Amazon (Amazon Web Services), Microsoft with the Azure platform, but within Europe and the Netherlands, there are also other providers offering cloud services. When cloud companies are small and only serve a limited number of businesses, the impact of an outage is relatively small. When services are delivered to a name registry or a bigger corporation, for example, an outage can have far more severe consequences.

A less known service is provided by the VERON organisation for radio amateurs. This service is called DARES, Dutch Amateur Radio Emergency Service and this group of volunteers help the Veiligheidsregio's (Safety Regions) and Ministry of Defence during severe communication problems [VER17]. Even though this service is actually not in scope of this research and is not a public service, it is deliberately mentioned as an example of how organisations can provide creative ways to help society.

4.5 Telecommunication architecture

The various telecommunication networks in the Netherlands have an architecture designed to cope with a wide range of functional and non-functional requirements. All these networks conform to certain architectural and design rules. In order to understand the technical issues with regards to laws and regulations, it is necessary to understands the basic architecture of telecommunications networks. This chapter describes the basics of networks and is based on a book on telecommunication networks [Fre99]. Having tried to use publicly accessible information from KPN, Vodafone, T-Mobile and Tele2 to enhance this chapter, it became apparent that these parties are not willing share information about their network architecture.

According to Freeman, telecommunication network architectures are split in a part providing access functions and another part providing core functions. The access functions enable customers and business to connect to the telecommunication networks, using fixed and mobile access technologies, while the core functions provide connectivity to services such as telephony, internet access and television services. This core network also provides connectivity to networks of other providers and enable world-wide interaction between people and systems. Worldwide connectivity is facilitated by satellite communications, submarine cables and underground cables. Each of these transport mechanisms has different specifications for confidentiality, availability and integrity.

Access networks are used to connect individual consumers and business to the services they need. Mobile networks use radio signals between the consumers and the base stations. Landline based services use twisted copper pairs, coaxial cable or fibre-optic cables for the last mile. Base stations can be connected to the core network using twisted copper pairs, fibre-optic cables and in some cases mini-links (micro wave for rural locations where it is not profitable to provide underground connectivity. When there were only

analogue telephone networks present, the local exchanges provided the power to the phones at customer premises (with the exception of the privately-owned exchanges (PABX). In the current situation, all equipment, such as residential gateways and set-top boxes, are locally powered. Power outages cause a disruption to all fixed services in the specific area hit by the power outage.

Another issue which can impact these local devices is when these devices are remotely managed and a fault in a configuration cause outages. For example this happened when a configuration error in the electronic program guide of KPN's set-top boxes rendered these boxes unusable until all these devices were updated with a patch[Sto14].

Fibre-optic cable and coaxial cable are the primary means for high speed connectivity, although techniques to improve communication speed over copper is being developed [Kro17]. From an economic point of view, improvements to copper network are useful for the service provider. From a continuity point of view, it cannot be determined what the consequences there will be if there is a slow-down in the roll out of fibre-optic cables [Joo17].

The mobile base stations are connected to the power grid. It is not known whether every operator uses power back-up equipment at every site where they operate. T-Mobile recently announced that they would upgrade their battery back-up from 30 minutes to a one hour capacity for their 5000 sites [Tel17]. As long as mobile base stations have a functional power backup during power outages, communication between base station and local access exchange buildings can continue.

The last mile of connectivity is basically a star shaped structure between the consumers and companies and local exchange buildings. Street cabinets placed between the two to form a distribution point. KPN mentions on their network information page that there are approximately 20.000 of these street cabinets in The Netherlands. (however there is not mention of whether all these cabinets are active and how power outages are counteracted) [htt]. In some cases, larger companies requiring high availability have their premises connected to multiple local exchanges to allow for local fall out and spread the risk of an outage. This is not standard practice. , There are approximately 1400 KPN owned local exchanges in the Netherlands but they may be used by KPN's competitors [Wik17]. The KPN corporate site states that there are approximately 160 metro-core locations (larger distribution point), which gives an indication of how the networks can be connected. Freeman states that basic network architectures use star-, ring-, or mesh topologies or a combination of the three. Given the 1400 local exchanges and the 160 metro-core locations, it is assumed that every metro-core location will serve a small number of local exchanges. The KPN corporate website states that there are ten datacentres, but the website does not specify how they are used [htt]. Based on the governmental report on a power outage in the Noord-Holland province, it is assumed that these local exchanges, metro-core locations and datacentres have adequate power back-up systems [Ins15]. This report also states that the 112 emergency service and the NCV (Emergency Communication Facilities) continued to function during an outage. This is a governmental requirement set for the network operator of these services, KPN.

Vodafone previously used an infrastructure with twelve datacentres. After the Rotterdam datacentre fire in 2012, it migrated to a three datacentre core network [Min15]. It is not known what the consequences were for the network architecture due to the Vodafone/Ziggo merger. The number of Datacentres operated by Vodafone/Ziggo and KPN gives an indication how services might be implemented at the top of a network. Based on the fact that Vodafone/Ziggo currently operates three datacentres, it is a given that all systems and service applications are fed from these locations. The remaining infrastructure (base stations, local exchanges) is in place to provide a robust connectivity between the customer and service applications.

From a network perspective, access to services must be possible. Each provider can be seen as a stand-alone network, with interconnections towards other networks (national and international)[Fre99]. If the interconnections fail between one provider and another, customers of the same provider can communicate, but no communication is possible outside of the providers network. Providers can choose

to interconnect through multiple connections to all other providers, however some providers may choose to limit the connections and therefore limiting the costs.

Connection between networks depend on protocols to facilitate service specific settings. Standardisation bodies help to determine these protocols. When the use of these protocols is abused, security is jeopardised [Too17]. In connected networks, a relationship of trust between all providers connected is needed to ensure that networks can be dynamically updated, expanded and changed.

After the Vodafone datacentre fire in 2012, the various providers co-operated to enable regional roaming between Vodafone, T-Mobile and KPN. Should a provider be facing problems, the other providers can provide temporary support to a number of customers of the troubled provider. Due to capacity issues, data services cannot be supported [Ned14]. For fixed telephony there is no such service.

International connections can be made using submarine cables, land-lines or satellite links. For phone communications satellite links can still be used, but their relevance for services such as internet is marginal. The World Economic Forum states that 99% of Internet traffic uses submarine cables for transport [Wor16]. An overview of current submarine cable routes is available on-line available [scm17]. This overview offers information of the cables itself and shows the landing stations for these submarine cables. Based on this map, the Netherlands has seven landing stations. The map does not show the internal European land based fibre-optic connections. Compared to other countries such as India, it can be said that the submarine cable connectivity is robust. India only has a single landing station but is a country well known for its outsourcing capabilities and yet so vulnerable in its robustness. The effects of a break in this submarine cable between India and Europe would have serious consequences, giving the amount of outsourced activities by Dutch companies..

For telecommunication services needing internet access, there are Internet-Exchange Points. These Internet exchanges have two main functions, one being to connect to other internet exchange points, thus creating a world-wide interconnected network. Secondly, to connect local service providers and companies to that worldwide network[Rya12]. For The Netherlands own critical telecommunication infrastructure, these internet exchanges are vital as they ensure communication both within the Netherlands and with other countries and continents.

Aside from the basic services provided by the telecommunications providers, there are also services available to customers who do not want to operate their own information system infrastructure. These services are called cloud services. Suppliers such as Microsoft with the Azure cloud and Amazon with the Amazon Web Services are some examples of such services. Alongside these American companies, there are also Dutch cloud providers delivering services from the Netherlands. Recently the company Randstad announced that it would migrate all its infrastructure to Amazon AWS [Spr171]. Having all services run from a cloud will create a higher dependency on telecommunication infrastructure. The datacentres where services could run from may be located outside of the Netherlands. An outage in a datacentre located in another country can have impact on services provided in the Netherlands. It must be noted that the larger cloud companies have multiple datacentres and geographical regions to minimise risk[Ama18] [Mic17]. When cloud type of services are provided by suppliers which can impact the critical infrastructure of the Netherlands, the Dutch government must determine and assign these suppliers, Operators of Essential Services, in accordance with the NIS. This must be done before October 2018. If this choice falls to the wrong company, this consequences can be major. An example is the DDoS attack on the Swedish transportation websites which caused train delays throughout their country [Bar16].

Another notable trend over the last decade is outsourcing of IT and infrastructure management functions. Service providers enter contracts with third parties which are required to manage the infrastructure on their behalf. These third parties can be located in other countries or other continents and are tasked with managing networks and services which can be critical to Dutch society. Finding recent information about these topics is difficult, but all three mobile providers have outsourced activities. T-Mobile has outsourced network services to Huawei [Bee14]. Vodafone has outsourced mobile network services to

Ericsson[AGC05]. KPN has outsourced IT services to Tech Mahindra[ANP12]. The exact consequences of these outsourcing activities is not investigated in this thesis. From a continuity and security point of view, it can be expected that detailed knowledge about how to manage these networks will at least partially transferred to the third parties managing these networks. It is also assumed that these parties have full control over the infrastructure they are managing for their customers. Based on the law on security clearance, employees having this type of privilege must have a clearance. It could not be determined whether providers are compliant with this law [Dut96].

4.6 Other services

Companies such as T-Mobile, Vodafone-Ziggo and KPN provide infrastructure services and content services such as TV. Content is not regulated by law and is provided by countless companies and by almost every individual who has connectivity to the internet. Over-the-top players such as Facebook, Twitter, YouTube and other social media networks distribute content generated by individuals and advertisers. This can lead to what is known as 'Fake news'. Certain companies buy advertisement space on Facebook and other social networks to spread news which sounds legitimate and logical, but is verifiably incorrect [All17]. Due to this issue playing a significant role in the last elections in the United States and during the terrorist attacks in the United Kingdom [Gri18], it is expected that the major OTT players will take action to prevent fake news. It may result in a government intervention. Whichever way, the consequences for the Dutch critical infrastructure are unknown. Further research into consequences is out of scope for this thesis, but is recommended. The Dutch government could order telecommunication providers to take Dutch sites off-line (there is a 'notice and takedown procedure for sites which discriminate or distribute illegal information [www08]). For sites which are considered harmful to Dutch society but are located outside of the Netherlands, other legal means are necessary if these sites are to be blocked. The verdict against The Pirate Bay shows how the legal system has dealt with this issue [Rec17].

4.7 Geographical issues

The geographical structure of the Netherlands also influences telecommunication services. The website of the Antennebureau (Dutch wireless communication registry) shows were antennae are located in the Netherlands [Ant171]. Based on this website it is concluded that certain rural areas are only supported by a very small amount of base stations, while communication in larger cities is supported by multiple base stations per square kilometre. This smaller amount of base stations can have a negative availability impact on rural areas, when coverage can be negatively impacted when just one base-station becomes unavailable.

Operator KPN has just started with a service to provide people living in rural areas with a multipath solution based on simultaneous fixed copper and 4G communications [KPN17]. Even though this solution does not mention continuity, services such as this may help to increase robustness of telecommunications infrastructure.

4.8 Services dependencies

As mentioned in paragraph 4.4, the list of critical infrastructures only mentions 'Internet access, Internet and data access and services' as critical services. Internet however is comprised of a variety of underlying sub services to provide basic connectivity, such as mobility management (to determine where a customer resides) and trust. For example, when a consumer wants to connect to his financial advisor, that customer might use a hyperlink to make that connection and will trust the certificates used to authenticate the website of the financial advisor. The consumer does not know that the hyperlink is translated to an IP-address using the Domain Name System (DNS). DNS uses a worldwide hierarchical architecture to ensure that connectivity can be established using logical names instead of arbitrary numbers, unknown to users of the internet. Issues with DNS have happened, and can cause unavailability for consumers and businesses [Hui17]. The DNS service consists of the global DNS services under management by ICANN [ICA17], and every country has its own Top Level Domain (TLD), such as.nl for the Netherlands. Registrars

and companies can maintain their own DNS implementations, serving their own customers and company. Domains are maintained by registrars and the entire architecture needs to be robust. Without DNS, communication over the world wide web is almost impossible, due to the amount of IP-addresses and domains available and the fact that alternative mechanisms are hardly known[ICA15].

The certificates used to make DNS more robust (DNSSEC, i.e. certificate based DNS), authenticate a website, person, document or institute are also part of a global architecture. Certificates are the mechanism providing trust for all aspects of electronic communications. The DigiNotar BV incident showed what the impact can be of compromised certificates on trust in the internet domain [Pri11]. Complexity of certificates and how they can be used is high, and maintaining integrity and security is a tedious business. Every Certificate Authority must provide a Certificate Practice Statement (CPS) which gives details about all aspects of these certificates. An example of a CPS is the Dutch root certificate CPS[Log16]. The complexity in governing these kind of services is high, due to the global nature, the number of stakeholders and players involved. The basic principles of certificate management are known to suffer from fundamental issues [Sch00].

4.9 When regulation clashes with technology

The rapid development of internet related technologies sometimes leads to clashes between lawmakers and technology. An example of such a clash is given in this paragraph, because it gives an indication of the problems lawmakers face when laws are made to protect consumers and society.

Every technology introduced will attract people with malicious intentions. Soon after the introduction of e-mail, the concept of spam was introduced, bothering people with loads of advertisements for a wide degree of products. This has led to the introduction of spam filters, both for mail clients running on the customers devices, but also on the servers used by the mail providers. These filters can be based on blacklists or whitelists, and are intended to remove most of the unwanted advertisements and are quite often based on the use of text and anomaly based mechanisms. For example, these filters can block messages containing certain words, or block messages coming from senders which have been defined as malicious. How these senders are defined as being malicious is out of the scope for this thesis, but there are mail reputation not-for-profit-organisations maintaining dynamic blacklists to ensure that filters are as accurate as possible [Spa17]. Looking into the content of a mail, other than by sender or receiver is a complicated matter, even to prevent malicious activity. The Dutch constitution, article 13, forbids communication providers to look into their customer's communication[Dut08], but these customers are also used to being protected and will complain when spam-levels are increasing.

Providers may block consumers which are sending spam, to protect their own services. Providers will be put on blacklists if their customers are sending spam, and therefore preventing other customers to send mail [Sec12].

When provider KPN announced that they were using Deep Packet Inspection (DPI) technologies, this caused an avalanche of events, from investigation by the Dutch Data Protection Authority, to national and European law providing net neutrality to European citizens [Rei11] [Sch12]. Due to this chain of events consumers within the EU can profit from net neutrality, but at the same time it is harder to prevent against the dangers of malware. Malware can be recognized by analysing DNS traffic (there are black lists available containing malicious domains) and by analysing network traffic by means of DPI to look for malicious payloads. Blocking this malware is beneficial to society, but care must be taken to ensure net neutrality compliance. The telecommunication law states that network operators must have controls in place to protect a network and malware detection can be such a control [Dut17].

In 2012, the American Congress passed a law stating that Chinese network vendors must be avoided as suppliers for critical services [Rog12]. The official reason behind this law is that American congress distrusts Chinese suppliers of telecommunications equipment. Dutch providers are also using equipment or services from Chinese providers [Bee14]. When backdoors are indeed present, these backdoors can be

used by attackers to manipulate, eavesdrop or block traffic. Given the fact that allies cannot be trusted as has shown by the British GCHQ [Gal14], it is recommended that providers use preventive and corrective controls to minimise risk.

4.10 Relationship and comparison with other sectors

The telecommunication sector must be seen in relationship with other sectors. Luiijf and Klaver have composed a model comprised of six elements which give an overview of the entire ICT landscape from OTT players and generic functions to the other critical infrastructure sectors using Critical Information Infrastructure (CII) [Lui15] Figure 2:

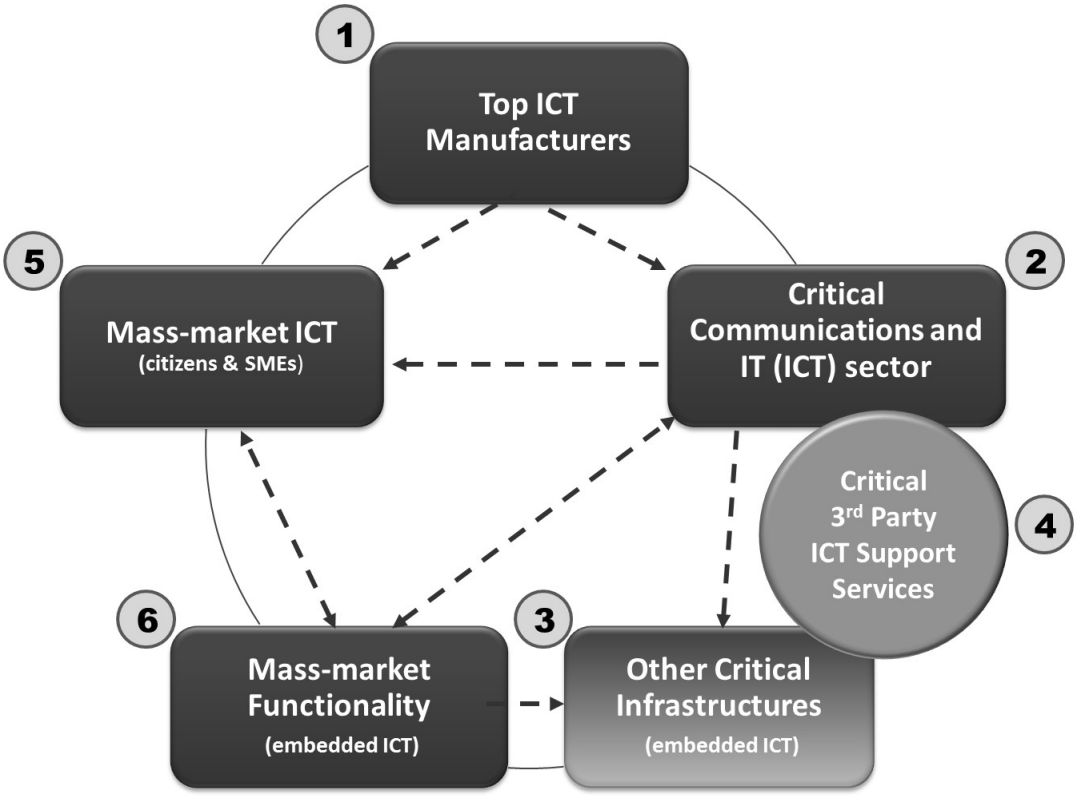

Figure 2 Division of the critical ICT infrastructure in six elements

The Dutch CII is shown as object 2 in this model. This sector is dependent on generic services such as DNS and certificates, mostly provided by the Top ICT Manufacturers, shown as object 1.

The other critical Infrastructures (object 3), consumers and businesses (object 5) are dependent on telecommunications. Suppliers of embedded ICT equipment are modelled in object 6. The telecommunications sector is cyclic dependent on the electricity distribution sector as has been mentioned. The critical ICT support services are mentioned in object 4. It can be seen that both the critical communications sector and the other critical infrastructures are using these support services.

In 2003, Luiijf, Burger and Klaver have performed a quick scan of critical infrastructure and came up with the picture in Figure 3 [Lui03]. This picture was designed in 2003 and that was a decade before the widespread use of mobile communications for IoT and telemetry networks. Smart meters, remote management of locks and pumps etc. have made the reliance on mobile telecommunications a lot higher than it was only 15 years ago and hence, if the graph were to be updated, would show a lot more dependencies on mobile communications. The telecommunication elements in scope of this paper are marked yellow.

As can be seen from this graph, there are many interconnections between the various sectors in the critical infrastructure and it must be noted than cascading effects will be experienced in case of serious incidents. Electric outages will have effect on telecommunication and both will have an effect on other sectors[Lui081] and [Lui08].

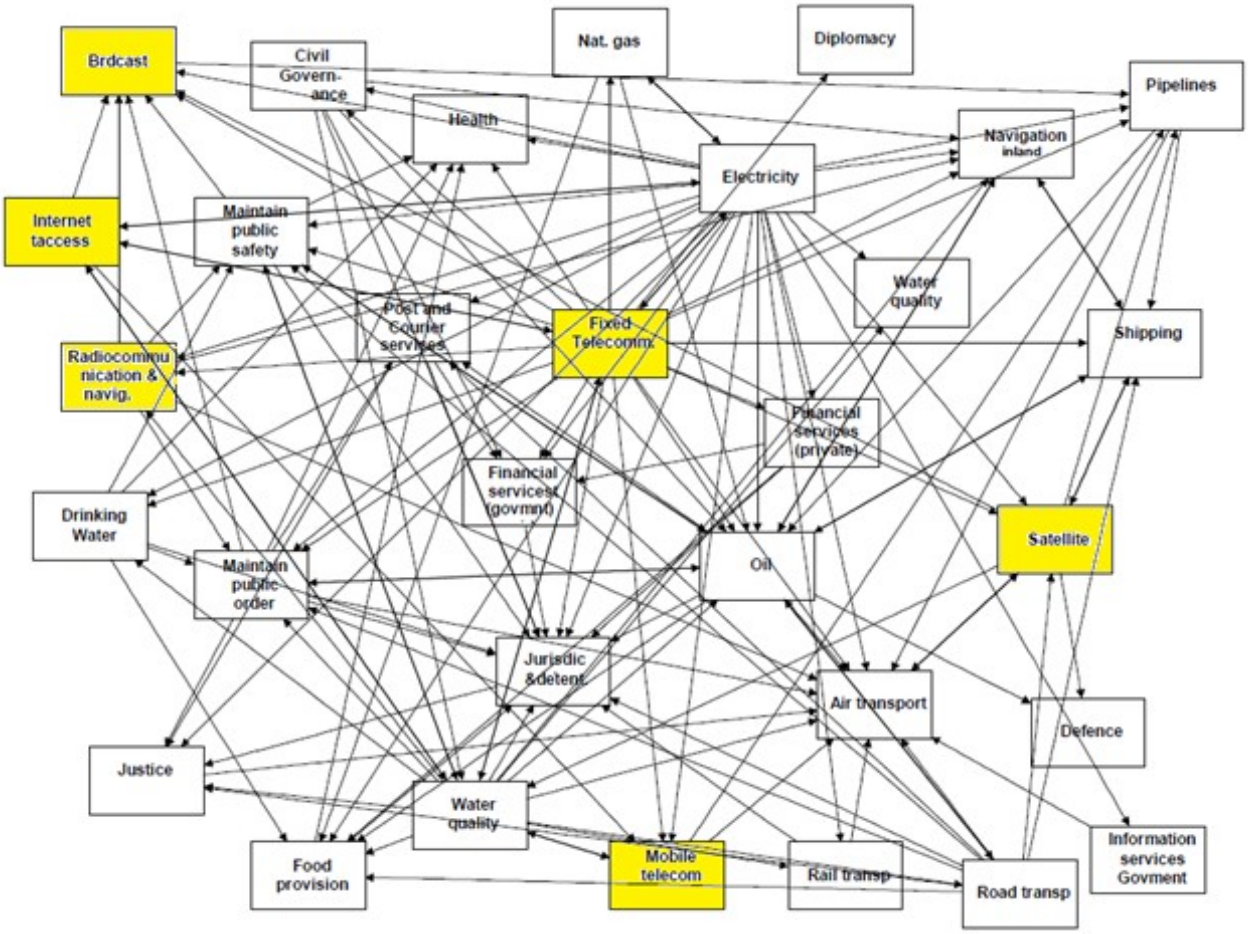

Figure 3 Infrastructure relationships (Luiijf, Burger, Klaver: 2003)

Looking at a more distant future, it is expected that the power grid will be less centralized, due to the development of more alternative electricity sources such as solar and wind power [Run14]. This can help to reduce the scale of electricity outages on a regional level, but it cannot be estimated how many years it will take before the majority of households in the Netherlands will be equipped with local means to provide electricity.

The various critical services mentioned are classified in an A and B category. On the website of the NCTV, it is shown what the selection criteria are to determine if an infrastructure is category A or B [NCT17]. The NCTV mentions a category A infrastructure as an infrastructure which can cause a death toll of over 10,000, have an economic impact of at least €50 Bn damage and causes emotional and surviving trauma for at least 1 million people. Next to these numbers, a category A infrastructure can cause a collapse of at least two other critical infrastructures. In order to be categorised as part of the category B critical infrastructure, the numbers are as follows: a death toll over 1,000, economical damage of more than €5 Bn and more than 100,000 people suffering emotional and/or surviving trauma. This difference in categories is defined to enable crisis management organisations to differentiate and set priorities during a calamity and to enable tailored workarounds and solutions in case of calamities.

The last updated list of critical processes, including backgrounds about the classification is published in the NCTV Magazine about national security and crisis management (Nationale Veiligheid en Crisis Beheersing) [NCT15] and kept up-to-date on the NCT website [NCT171].

An interesting comparison can also be made with the banking sector, even though most banks are private sector institutions, whereby every country has a national bank, such as De Nederlandse Bank in the Netherlands. This national bank must ensure financial stability [DeN17]. The banking crisis of 2008 showed that even though controls were in place to ensure stability, continuity was impacted [Del10]. The national governments had to financially help the larger banks, which became “too big to fail”, to prevent a financial meltdown [Kau13]. When this is translated to the telecommunication sector, the government must prevent that failure of one service provider has catastrophic effects on other service providers and on availability of essential services for Dutch society.

From a legal perspective, it can also be noted that regulation of the telecommunication sector is similar to regulation in the banking sector. The law on financial oversight [Dut06] has chapter 6 devoted to the stability of the financial sector. This chapter is written to ensure that the critical infrastructure of the banking systems is guaranteed.

The electricity and gas sectors have different regulations. Both the electricity law [Dut98] and the gas law [Dut001] distinguish between production and transport/distribution companies. The government assigns companies for a period for ten years to manage and operate the transport and distribution facilities for electricity and gas. These transport and distribution companies ensure that gas and electricity are delivered to the consumers.

With regard to drinking water, the country has been split up in regions. Every region has a single private company producing and distributing drinking water to the consumers [Dut09]. For both electricity/gas and water sector regulatory oversight is provided by the government and also notification obligations are stated in the applicable laws. Availability requirements for critical services are not quantified, with the exception of drinking water supply.

The telecommunication sector has the NCO-T where continuity related topics are discussed. Other critical infrastructure providers have direct communication lines with the Department Crisis Centres (DCC) of the responsible governmental departments. Other sectors have sector specific organisations such as VEWIN for the water sector[VEW17] and Netbeheer Nederland for gas and electricity distribution [Net17]. This last organisation shows the average availability for the last five years on its website. These sector specific organisations help with common topics and issues within a sector. Available laws and regulation has not shown how inter-sector communication takes place.

A thorough comparison of the availability and security of critical infrastructure between countries could not be found in scientific literature. An interesting overview was found on the website of statistics provider Statista [Sta171]. This page shows Switzerland as the number one ranking country, and Netherlands as number 5 on a global level. Within the European Union countries, the Netherlands ranks first. This website states that all infrastructure is taken into account, such as road- and waterways, ports, airports, telecommunication, power grid etc. More detail about specific telecommunication infrastructure could not be found researching publicly available information.

The company P3 publishes annual performance benchmarks for mobile communication. These tests are performed in multiple countries and measured in such way that countries and operators can be compared. The tests are performed by driving through 17 large cities and 19 smaller towns in the Netherlands, as well as the connecting roads in between [P317]. Operators can obtain a maximum of 1000 points and the average for the Netherlands is 934 in this report. P3 has determined that the chosen area is representative for where most of the Dutch people use mobile telecommunication facilities. Based on these tests the mobile operators can determine their strategy to improve their networks. Companies which are sensitive for the numbers as presented by P3 might choose to improve their services in the areas covered by the P3

tests and neglect other areas. When compared to the 782 average in the United Kingdom in 2016, quality and coverage in the Netherlands are very high[P3C16]. This difference can also be found in the Statista infrastructure ranking [Sta171], where the United Kingdom ranks 28.

Due to the fact that these tests only focus on a small part of the Netherlands, it gives incomplete results, with regard to coverage in rural areas and towns other than the ones used in the tests. From a security point of view, coverage is necessary in the entire country. When operators decide to only improve their networks in the areas tested, this can lead to a lower level of service in other areas. The test further put emphasis on data speeds, which are based on available spectrum, and do not take robustness of a network in mind. Continuity of service is not a part of the P3 report.

4.11 Privatisation in the Netherlands

Over three decades ago, most of the Dutch critical infrastructure was owned and managed by the Dutch government. Since the late eighties, privatisation of infrastructures and services has taken place with various results and consequences as described by a report of the Dutch House of Representatives[Eer13]. This report is used as main source for this paragraph.

Privatisation was chosen as a method to decrease the size of the government, in numbers and in budget needed. An added benefit was that it was expected that a privatised organisation would operate in a more efficient and customer friendly way. The report states that these privatised companies have built new relationship with consumers and governmental institutions, but that even though relationship between those companies and governments is more distant, there is still a struggle on how to regulate these companies in such way that the markets they serve, will not become defunct (due to monopoly of the incumbents etc.).

The Dutch telecommunication sector was the first one to be privatised, because it was foreseen that an institute under strict governmental control could not operate in a rapidly changing market. With hindsight, this is according to the author of this thesis a good foresight by the governments at that time. Besides being privatised, the incumbent PTT also ownership was transferred on the stock exchange market in 1994. With later privatisation projects,, such as with the Dutch Railways and the Electricity sector, the infrastructure was kept under close government control, while the service provider roles were privatised. When KPN (then PTT) was privatised, KPN did obtain the infrastructure as well as the services. Even though the original law on privatisation ordered KPN to split up the company in a concession part and a commercial part, an adaptation of the privatisation law allowed KPN to continue as a single business entity [Mai93]. In 1998 the post and telecommunication company was split up in separate post and telecommunications companies [Jor98].

The Dutch railways were privatised, for the same reasons as PTT, mainly to enable the privatised institution to work in a more efficient way. In a later stage, also competition became a topic of discussion and was implemented in further steps to be taken. Other governmental institutes such as the Social Insurance institute (Sociale Verzekeringsbank) were privatised, but kept their monopolist role.

The government did not manage to reduce the headcount and finances involved according to the privatisation report, due to complicated communication lines and government and the effort required to keep society balanced with regard to the critical services required.

The privatisation report of 2013 has defined five recommendations to improve understanding of and dealing with privatised institutions and for future privatisations[Eer13]:

1) Consistent definitions of terms, to make privatisations comparable and prevent confusion in discussions.
2) Compact and consistent decision-making process guidelines, to improve decision making.
3) Uniform rules and regulation, to improve governance

4) Make one governmental department responsible for all governance with regard to privatised institutions.
5) Periodical political review, based on regular governance reports.

In order to improve governance over privatised organisations the following recommendations have been made in the Senate report:

6) One secretary-general is responsible for privatisation decisions and will discuss his decisions with the board of secretary generals.
7) Better controls to govern, audit and monitor privatised institutions. Examples are:
    a. Audit whether policies and management goals of privatised institutions match.
    b. Market analysis to determine market needs with regard to regulation, governance, impact and effectiveness of current controls.
    c. Independent and effective governance to ensure that the needs of the various stakeholders in a market are balanced.
    d. Evaluation of processes and results in a market. This is already a requirement, once every five years, but this requirement must include a check whether the chosen form of privatisation still suffices or need to be reconsidered.

The Senate report also deals with recommendations for the House of Representatives and Senate, of which recommendations are mentioned here:

8) Improve level of information for decision making within House of Representatives and Senate.
9) More attention for operational effects of policy making and the monitoring thereof.
10) 2nd chamber of parliament must involve the Senate on an earlier moment in time in case of proposed privatisation.
11) Temporary commissions must be established in case of privatisation proposals, to optimize processes and governance of privatisation proposals.
12) Better insight in effects of EU regulation, to optimize privatisation efforts with regard to EU laws and regulations.

The Senate report also states that the benefits of consumer stakeholders are not sufficiently met and improvement can be made using the following recommendations:

13) Laws must be defined for every privatisation project to ensure that every stakeholder has a clear view of benefits and consequences.
14) Assessment of public interests and consequences of an intended privatisation in order to obtain the right balance.
15) Direct reporting from executive officers of privatised companies towards parliament about the privatised institution and the way the institution is managed.
16) Improved horizontal compliance and reporting from privatised institution towards other stakeholders such as consumers, suppliers, and competitors to improve transparency and compensate for decreased governmental insight in operations.
17) Clear and easy means to complain for consumers, competitors, and suppliers for privatised organisations which do not operate in an open market.
18) Better information towards citizen about privatisation processes, the transfer periods and how operations will be run in the new situation.

In chapter 8, of this thesis certain items mentioned in these recommendations will be addressed.

5 Actual cases

This part of the research does investigate whether laws and regulations were sufficient to counter threats encountered in some cases which caused the Dutch government to respond. Three cases have been

selected, one which had a technical impact on society and another case which could have caused regulatory control issues for the Dutch government. The third case happened during the research for this paper and was caused by an Apache helicopter cutting power grid cables and causing a regional power outage. The first case is known as the DigiNotar case, while the second one did involve KPN when this company was almost taken over by Mexican investor Carlos Slim. In all three cases, it is investigated whether laws in place were adequate with regard to the threats which the government wanted to avert.

5.1 The DigiNotar case

DigiNotar BV was a Certificate Authority (CA), and provided digital certificate services to notaries, the Dutch government and other customers. Mid 2011, it became clear that the DigiNotar certificate services were breached, probably by Iranians and that fake certificates were issued [Pri11]. This breach caused worldwide attention. All major browser vendors removed the DigiNotar public root certificates from their browsers, in order to restore trust. The Dutch government intervened and took over control of DigiNotar BV, after threatening with a short action law suit[Don11]. There is no literature available stating the articles of law which would be used to file the law suit, due to the DigiNotar parent company Vasco agreeing with the take-over. The motivation to take over was based on lack of trust on security and concerns about economic security [Pri111]. After the problems were solved, DigiNotar BV went into bankruptcy and the certificate business has been taken over by various companies. The DigiNotar company was not part of the Dutch critical infrastructure, even though from a financial point of view, strict regulations applied. The impact of certificates was underestimated before the DigiNotar hack, and the impact of the hack was felt world-wide[Wol16]. Even though certification was a necessity and DigiNotar was certified by a well-respected auditing organisation, the internal procedures were flawed and attackers have been able to falsify certificates [Pri11]. Since 2016, the Agentschap Telecom organisation audits certificate and identity providers to prevent incidents such as the DigiNotar case to happen again[Age17]. Given the fact that fundamental issues with certificates have not been solved, even though these risks were published in 2000, it is hoped that new incidents will not occur [Sch00]

5.2 KPN ownership case

Mid 2013, the Mexican company América Móvil showed interest in taking over KPN. This would mean that KPN shares would all be owned by a Mexican company. Within Dutch government and in society, there were concerns about continuity and security of the services provided by KPN. These concerns culminated in the KPN protection foundation taking 50% ownership of KPN using Class B preference shares [Fou13]. Although a danger of a hostile takeover was averted, the Dutch government was concerned that such a take-over attempt could happen again. The Dutch government has made proposals to prevent hostile take overs concerning critical infrastructure [Ka017]. At the moment of this thesis, a specific law to protect Dutch private institutions with respect to foreign take overs is not yet in place, although consultations have taken place [www17]. Various parties including KPN [Dav17]and Confederation of Netherlands Industry and Employers [Dri17] have already made objections and suggestions. The KPN chairman made it clear in the article by Bremmer that government influence must be avoided to ensure the free market and competition will function. He argued that the protection construction of KPN worked well to avert the threat of the hostile take-over. Drion argues that government oversight is actually good to protect critical infrastructure, but that laws to protect the telecommunication infrastructure should reflect practices in place in laws for the governance of electricity and gas transport networks and the law on financial oversight. The electricity and gas markets however, are not directly comparable, due to the fact that these infrastructures are shared between multiple operators whereby the government assigns an operator for the infrastructure itself for ten years periods. The financial market is more comparable due to the fact that each financial institute must take care of its own infrastructure.

With the current state of laws and regulations, this kind of take-overs can’t be prevented, other than by means available, such as the Foundation Preference Shares in case of KPN.

In 2017, the Nijmegen university published an extensive report about foreign take overs of private sector institutions. In the conclusions of this report, the authors stated that hacking probably would present a bigger danger than foreign ownership [Bul17]. They did not know whether critical services such as 112 and C2000 could easily be transferred from one operator to another operator.

The Dutch military has specified regulation to ensure that companies delivering services to the Dutch military will not compromise national security. These are the ABDO (Algemene Beveiligingseisen Defensie Opdrachten, or General Security Requirements for Dutch Defence Assignments) [Mi017] The ABDO-requirements must be adhered to by companies working for the Department of Defence. One of the ABDO provisions is the clearance obligation for contractor employees working with services or equipment, meant to be use by the Dutch military. Even though this regulation states requirements with regard to ownership of a company (must be reported and assessed), this ABDO can't prevent a take-over. Only the business with the company which has been taken over can be ended, because of the risk to defence security.

5.3 Apache helicopter power supply interruptions

During the writing of the thesis, the writer of this thesis happened to experience first-hand what the effects of loss of telecommunication can cause. In the evening of November 13, around 19:00, 2017 an Apache helicopter of the Dutch Army cut a high voltage power line causing a power outage.[Vei17]. Approximately 24,000 households in the Tiel and Culemborg area of the Netherlands were out of power until around 00:30 the following morning.[Vei171].

A remarkably similar incident happened December 12th 2007, when an Apache helicopter cut a high voltage line over the river Waal. Restoring power took three days, and over 50.000 households were affected.[Luc17]. The Onderzoeksraad voor Veiligheid (National counsel for security incidents) has performed an investigation with regard to the root-cause. The aftermath of the accident was not part of this report [Ond09].

The helicopter caused an immediate power outage. Fixed telecommunication services were instantly gone. Mobile services were still working depending on the operator. Depending on the operator, loss of mobile coverage was experienced in within a couple of hours. The author of this thesis happened to be in the vicinity of a base station just outside of the area hit by the incident and did not experience any outage of mobile services. However, performance degradation was obvious and fall backs from high speed 4G to slower H+ and 3G services were regularly experienced.

The Safety Region Gelderland Zuid, responsible for crisis management in the region did report about the incident on their Twitter account (@CrisisGLZ) at 19:59. Their website stated that indeed an incident had happened and that information was published on the websites of the power-distribution system operator Liander and CrisisGLZ [Vei17]. This information was only available to people outside of the affected area and people having smartphones with working connectivity.

The Veiligheidsregio advised people at 21:06 to unplug electric equipment to make a restart of the grid easier and prevent damage to consumer equipment. The writer of this thesis argues that the advice might have been better to just switch the mains off with a single action, instead of having to pull plugs for every device. This will ensure consumers will not forget individual devices. It is not known whether telecommunications providers planned to use or used generators to reduce the outage. Two minutes later, it was requested to only use mobile phone communication in case of necessity. At 21:24, it was advised to listen to Radio Gelderland for updates on FM radio. It must be kept in mind that only battery powered radios or car radios could be used by people in the affected area. At 22:32, the public 14024 helpdesk phone number was activated for people having questions. At 23:11 the CrisisGLZ tweeted that cars equipped with loudhailers were informing citizens about progress. These vehicles were not heard in the neighbourhood where I live, and people in this neighbourhood did not know what to expect with regard to the outage timelines. At 23:55 Liander (@LianderNL) tweeted that they expected that power would be restored around 00:30 the next morning.

The author of this thesis, nor people in the same neighbourhood have received any NL-Alert messages, although the Veiligheidsregio website explicitly mentions the use of NL-Alert during power outages [VGR17]. The same page also mentions that 112 will always work due to a specific emergency network for this service, but the author of this thesis dares to argue that this claim is not true. The 112 services use the same mobile and fixed networks as other telephony services as has been demonstrated in the Diemen power outage of 2015 [Age17]

At 21:08 a neighbourhood watch WhatsApp message was received confirming the Apache incident with recommendations from the local police. The police requested members to take a stroll outside to patrol and hence, be vigilant and alert to help the police. In case of emergencies, neighbourhood watch members must call 112. The police was already patrolling more and had at least one helicopter on air above Culemborg since approximately 20:00 in order to prevent burglaries and other incidents.

The website of the Veiligheidsregio Gelderland Zuid has a page about their alerting procedure in case of crises. This procedure mentions the use of a regular phone for communication [VRG17]. It is not known whether this method has been used to alert the people necessary to combat the crisis.

In the evening people were seen in cars, listening to emergency broadcasts by the regional radio station as Twitter and Internet-based feeds were unreliable for most people. Where I live most households don't have access to battery powered radios anymore. If this situation would be representative of the entire Netherlands, this will impact the effectiveness of government communication in case of power outages.

Based on conversations with other people living in the same neighbourhood, most people took the conditions easy. Not many people did get the twitter and web-based information, or did spent much time listening to radios. The people in the neighbourhood I spoke to, confirmed my own ideas that people would wait till next morning to see whether extra action would be necessary to counteract the effects of the power outage. I wonder what might happen in scenarios whereby drinking water delivery is stopped for a couple of days, or a flooding of less than a meter is experienced.

The ways of crisis communication by involved governmental and electricity company stakeholders was surprising. The Security Region must have ideas how to reach most of the people affected. The outage was, given the expectations of the previous incident, solved in a rapid way. How would the area affected deal with no power and hardly any telecommunication facilities for a prolonged outage? Electronic payments are not possible, alarm systems will become useless, due to lack of mobile communications, just-in-time provisioning of grocery stores will not work, health care services at home can get interrupted, warming houses and water will become a problem for most of the people and businesses involved.

6 Preliminary conclusions based on desk research

The security and economic lenses as have been defined by Veen and Dunn have been used to see whether the laws and regulation in place are indeed effective with regard to the protection of this critical infrastructure. The views are overlapping in most aspects, and according to the authors, the government shall always have to balance security and economy, to prevent excesses in either way.

In essence, the regulation is sufficient according to the authors, given the high availability of critical telecommunication infrastructure. The Agentschap Telecom yearly report over 2016 reports 57 incidents, however it can't give a good indication over actual availability[Age17]. A general figure can't be given due to the variety of incidents and the fact that providers have some liberties as what they report with regard to smaller incidents[Age17]. There is a minimum requirement with regard to what must be reported but multiple operators report more than what is required. These minimum requirements are based on impact on 112 services and the amount of consumers interrupted. The AT report of 2016 reports that the availability of services is high. In combination with the Statista report [Sta171] which reports the quality of Dutch infrastructure with a global 5th place ranking (see chapter 12 for the top-30 of this list) , it can be assumed that regulations are sufficient and effective from a government perspective. Readers can ask

themselves if this is due to the regulation or that competition between providers and market demands are also a cause for high quality services.

6.1 Economy versus continuity

Communication during a crisis is important. A lack of information provided by governmental authorities will lead to assumptions, and will impact society as has been shown with the Apache incident [Eld17]. From a security point of view, the government must ensure that people can be informed in a quick way. Based on the experiences of Eldik and my experiences, people had to use their car radios to get informed about the power outage. With most people using FM radios, it will be an interesting case when the government decides to stop using analogue FM broadcasts. Even though there are no official dates set, it is expected that Digital Audio Broadcasting (DAB) will replace analogue FM as a technology. It is not known whether the government has taken the turn-over of car radios into the equation for the transition from FM to DAB. Given the current penetration of DAB radios with only 6% of people in the Netherlands, this can lead to a lack of information after FM frequencies have been switched off [Kis17].

From a regulation perspective, it is observed that all critical infrastructure providers have to apply strict controls to ensure a high availability, and in case of problems, operate an effective crisis management operation. This may lead to heavy investments from critical infrastructure providers such as telecommunication service providers. Investments will have to be paid by consumers eventually by increased subscriptions etc. Consumers and institutions are well used to the levels of availability of the Dutch telecommunications services and do not expect outages. Hence, not many consumers and institutions take precautions to ensure that in case of longer lasting outages business can continue in whatever way possible.

Externalisation of risk is seen as a structural problem. In order to improve robustness, telecommunication might have to make changes to their network architecture. The investments needed for these changes will ultimately be paid for by the consumers of these services. It can be questioned whether customers want to pay more for services, even if the government orders the providers to make improvements.

The website of Agentschap Telecom has information about the Telekwetsbaarheid program to improve awareness to society that telecommunication might be unavailable in case of crisis [Pro17]. The Apache incident of 2017 however showed that people are not prepared for outages, even for a relatively short duration. When people are prepared for emergencies, the effects are perceived as less severe, by increasing the circle of influence at the cost of the circle of concern.[Cov89].

Even though the message is a difficult one to bring, there is a need for the government to prepare consumers and institutions within the Dutch society for crisis whereby communication may be disrupted. Better awareness will enable people to set their own risk appetite level and act accordingly. Governments and private institutions don't have to invest to add a couple of tenth of percent's to availability figures which belong to the highest in the world [Sta171] A risk-less society does not exist and would not be financially sustainable, although every solution to this wicked problem will introduce new problems.

A raised level of awareness will help consumers to make their own plans to counteract crisis by providing alternatives. For example, if consumers, companies and institutions would have portable power generators available, that will help by continue to use communication facilities. It must be noted that power generators must conform to governmental regulation [Dut071] due to storage and use of fuel. Running a power generator without a proper exhaust can cost lives due to carbon monoxide poisoning.

Laws and regulation focus on the process aspects of continuity. All laws in place, from both European and Dutch perspective focus on 'appropriate controls', availability of experts within organisations and process related topics such as business continuity plans. This is not only the case in the telecommunications sector, but also in other critical sectors. There is not any quantifiable number with regard to availability of services stated in the law. Only for the 112 service, an older government web site states that the availability of the 112 service has always exceeded 99,9% [Rij13]. The Agentschap Telecom report about

the power outage in the North of Holland reports that the 112 outage did last two hours[Ins15]. The report about the outage in 2017 states that the average waiting time for a 112 call should be 10 seconds for 80% for all calls[Ins17].The law does not set specific requirements with regard to service availability and also providers do not publicly share information about availability of their networks other than that availability cannot be guaranteed and that availability is as high as possible.

Even though availability of telecommunication services is “all-right” according to Agentschap Telecom [Age17], it would help consumers, institutions and governments if actual numbers of performance would be available. I argue that consumers and institutions can base decisions for emergency controls (power generators, using subscriptions to multiple providers etc.) on the availability figures as stated by the various providers. Better knowledge about possible risk, also reduces the fear of that risk. Availability comparisons of Telecommunication services worldwide have not been found

The privatisation recommendations mentioned in paragraph 4.11 give a multitude of suggestions with regard to privatisation efforts and governance of privatised institutions. I would not recommend to make one department responsible for governance of all privatised institutions given the wide range of possible sectors these institutions operate in. Using standardized ways of governance and reporting is however indeed recommended. In market analysis, it is important to not only take competition and other economic motives into account, but also security and continuity of the market segments where the privatised business operates. Recommendation number 15 is also an interesting suggestion: Let executive managers of privatised companies (and other major players in the same market, in order to keep competition fair) explain to the House of Representatives what is done at a high level to conform to laws and regulation from continuity and security perspectives. This also will give the policy makers more insight in risk appetite and ways of working in the various market segments.

With the privatisation of KPN, it was expected that the part of KPN, responsible for the operation of critical infrastructure would be nationalized again. Already in 1993 it was decided not to continue with this intention [Dut93]. The larger service providers in the Netherlands, don’t publish information about their intentions with regard to the operation of networks. I decided not to follow up on possible consequences and opportunities, due to the fact that this is an extensive research project in itself.

After the UMTS auctions in 2001, the former regulatory bodies Opta, NMA (OPTA and NMA have become ACM) and AT have written recommendations to make co-operation possible between operators. These recommendations had a strong focus on anti-trust regulation and ensure that consumers rights would be respected. It is advised that a new analysis be made, taking not only competition effects in consideration, but also focus on possible co-operation to enhance continuity and security of the services offered.

6.2 Economy versus security

Based on the experience gained during the power outage caused by the Apache helicopter, it was surprising to experience that the Veiligheidsregio, the power grid company Liander and other news sources continued to use Twitter and Facebook for communication purposes. The Veiligheidsregio even mentions Twitter as their official channel[Vei172]. The WhatsApp neighbourhood watch groups also continued to communicate. The NL-Alert has not been used by the Veiligheidsregio, even though this could have been a quick way to inform all households within the first half hour after the incident started. Author of this thesis has hoped to interview a representative from the Veiligheidsregio, but this request was not acknowledged due to time constraints on their behalf. It is suggested that more attention can be paid to the use of the loudspeaker-equipped cars to inform society in case of outages.

The widespread use of Facebook, WhatsApp and Twitter is also a cause of concern. These OTT players have so many people using their services and their services are used all over the country. Even though governmental bodies use these services as a way of communication, there are no policies governing the use of these services by governmental and private institutions in case of crises. This leads to the following questions:

- How can the Dutch governmental institutions obtain the same situational awareness about situations in the Netherlands as these OTT players have? The OTT players have a better situational awareness about society than a government can ever have, based communication patterns in twitter etc.. This makes the reader wonder about questions such as (but not limited to):
    - Does WhatsApp have insight in actual information shared with WhatsApp neighbourhood watch groups?
    - Will the government have access to detailed information obtained by these parties?
    - What will be the financial impact of obtaining this information?
    - Will regulation be possible by ordering these OTT players to share this information with critical infrastructure providers and the governmental departments involved in governing critical infrastructure?
    - Is this information also used by insurance companies to determine whether households in certain areas have to pay higher premiums?
- What is the official government view on using these channels for official communication by the government and critical infrastructure providers in case of crises?
    - Due to the fact that these communication channels are used by default, how can people be informed who do not have internet access? (this problem is getting smaller and smaller each year).
    - How to use these channels to communicate to society when these channels are not trusted, due to 'fake news' labelling.

Even though part of these questions falls outside the scope of this research, these questions are worth further research.

The Dutch government is well equipped to fight security issues with regard to critical infrastructure. A well-defined and organised crisis management organisation is a foundation for a speedy recovery in case of a crisis. From a competition point of view, co-operation is not always possible, without conflicting anti-trust laws and regulations. However, in case of attacks with an impact on society, co-operation is still possible and additional laws do not seem necessary. It is hoped that a crisis organisation can help to ease pressure and keep communication open.

6.3 Economy versus the combination of security and continuity

The DigiNotar crisis has shown that the government has enough capabilities and formal laws to ensure that in case of emergencies, the government can take control of businesses. It is assumed by the author of this thesis that directions issued by the government to telecommunication providers are also sufficient to reach the means society needs.

Division of critical infrastructure in a class A and B is arguable with regard to the categorisation of telecommunication services. The division is made based on an envisioned amount of victims and the economic loss. These two criteria are considered to be convenient to determine whether a service is category A or B. Given the rise of impact with regard to the use of telecommunications, it is suggested to have the telecommunications sector assigned as a class A infrastructure, for at least the internet access and data services part. With all aspects of society making an increasing and heavy use of telecommunications, outages and disruptions will have a high impact. Scenarios such as hospitals being DDoSed[4], or using cloud based services for patient registration and processing of all kinds of health-related data, being hacked pose a risk for society. Disrupting these kinds of institutions can cost lives. It is expected that some of the larger hosting companies will be designated as Operators of Essential Services according to the NIS directive.

4 Distributed Denial of Service, an attack whereby availability of services is impacted.

Based on the current discussions about telecommunication infrastructure and the current proposal to adapt the laws with regard to hostile take-overs, it is seen that telecommunication service providers are confident that no extra controls are necessary as is demonstrated by an interview with KPN CEO Eelco Blok:[Dav17]. KPN however, has been protected against a hostile take-over by a Dutch foundation in 2013 [Amé16]. This take-over attempt was the main motivation by the Dutch government to make additional law proposals[Kam17].

The proposed law which can prevent hostile take-overs can be seen as a good mechanism to ensure that continuity and security of critical processes and services are not hampered. From the point of view that a state has to provide security, this law can be seen as a necessity. Author of this thesis agrees with the Confederation of Netherlands Industry and Employers VNO-NCW secretary that the government must ensure that a level playing field exists, whereby all stakeholders know what to expect [Dri17]. Drion does not mention drinking water supply, which is based on regional companies, each having a monopoly in their region. The sectors gas, electricity and banking as mentioned by Drion have similar regulation requirements with regard to continuity and security, but have completely different stakeholder balances. In the telecommunication sector, there are many more different parties involved. Most of the infrastructure is not shared with the exception of some services such as the C2000 network and 112 network and the number portability database as managed by COIN[Sti17]. Author of this thesis argues that it will not help society if certain parts of the infrastructure will be managed by a single party to be assigned by the government, however, more co-operation between sectors from a government perspective would be welcomed. As per today, only the telecommunication sector has an NCO. The communication lines between the other sectors have not been investigated in depth.

Based on the aggressive stance of state sponsored state cybercrime (e.g., Russian influence on elections, [AIV17], it can be expected that also from a European perspective laws and regulation may be adapted to ensure a high level of security for telecommunication infrastructure. In special cases, the Telecommunication law, chapter 14 directives may be used to block certain traffic to prevent these kinds of attack. This can be seen as an extension of a ‘notice and takedown’ procedure which is used to fight racism, discrimination, hate speak and child porn. Expansion with other categories is a sensitive topic, due to the fact that filtering can be associated with censoring.

An underlying issue which needs attention is the amount of outsourced activities. Although authors have not been able to determine exact numbers and roles of functions being outsourced by providers, the impact can be high in case of security and continuity incidents. Most of the sources mentioning outsourcing are older, and no information is available about current state. Only the ABDO regulation has provisions about how to deal with defence suppliers which outsource activities. From a critical infrastructure perspective, the author of this thesis suggests to further analyse risk and other issues associated with outsourcing to determine whether additional controls are necessary. The parties managing the networks for the providers can have more control over infrastructure than majority shareholders.

7 Qualitative research interviews

The desk research has given insights about applicable laws, stakeholders involved and about the interactions between stakeholders with regard to the critical services in the telecommunications sector. In order to validate the primarily conclusions, interviews were held with s small number of people working in various areas of the landscape. The people interviewed have key roles within organisations involved in law and regulation aspects, or perform key roles in providers. Hence the information and opinions obtained from these people is considered to be representative of the organisations they represent. Also a couple of consumers of services have been interviewed.

The interviews have been conducted using face-to-face sessions. The notes taken during the interviews were shared with the interviewees, to ensure that the notes would accurate reflect both the outline and

details of the interviews. The interviews were conducted in a semi structured way, using open questions based on the following short list:

- What do you think about security and reliability of Dutch telecommunications infrastructure (fixed and mobile telephony, internet access and other connectivity services)?
- Which parties are responsible to protect this infrastructure?
- Wat is your definition of effective in regard to effective controls to protect critical infrastructure?
- Are you aware of the role the government plays with regard to protecting this infrastructure?
    - Are government controls effective in your opinion?
- What needs to be done to properly protect this infrastructure according to your views?

Based on the answers on these questions, follow up questions were asked to elaborate upon the information and opinions given. The interviews were planned to last approximately an hour but most interviews did take over ninety minutes to complete. The interviews have been organized based on the stakeholder role of the people interviewed. Using this order has proven to be the most helpful in categorizing issues with regard to effectiveness of laws and regulations. Exact quotations are not used, due to the delicate nature of the topics. I have decided to describe the essence of the interviews in the various paragraphs without compromising stakeholders and stakeholder interests, in order to assist in the continuous effort by all stakeholders to improve robustness and reliability of the Dutch critical infrastructure.

7.1 Government as Regulator

From a governance perspective, multiple parties are involved with regard to audit and regulatory oversight of telecommunication service providers, each with a different focus. The ACM has the focus on anti-trust and economic aspects of sectors and markets, the Dutch Data Protection Authority AP (Authoriteit Persoonsgegevens) has a focus on privacy and AT (Agentschap Telecom) has a focus on security and continuity.

From the regulator's perspective, auditing service providers based on the term "appropriate measures" according to article 11 of the Telecommunication law poses difficulties. When are measures appropriate? When are providers lagging behind? These are questions the AT is faced with. The regulation with regard to continuity of telecommunications gives some more guidance, but only related to providers having to have continuity plans, regular risk assessments, having experts available [Bes12]. AT has provided telecommunication providers with a document to assess what a continuity plan should contain [Age].

Even though the availability of infrastructure is high according to the regulator, it is hard to determine whether this is due to the laws and regulation in place, the AT audits, or just because of the competitive telecommunication market situation. There are agreements about reporting incidents involving outages for customers (above a certain threshold). Serious incidents always have to be reported, also less serious incidents are sometimes reported. The purpose is to evaluate these incidents and see if continuity aspects can be improved.

After five years of having received reports of incidents, AT has evaluated the obligations of telecommunication providers to report incidents, to see whether certain controls could be improved. The purpose was to see whether lessons could be learned from incidents and whether incidents can be used to give insight into the degree of continuity. The evaluation did not yield clear usable results. The critical infrastructure providers also have evaluation programs in place for these kind of incidents. These evaluations are not shared with AT or other operators. It is expected that the internal follow up within telecommunication service providers already helps to prevent high impact incidents. In 2015, AT has started a project with the Twente University to see if a model can be developed to use reported incident data for risk analysis [Cen15]. Their project LINC (Learning from Incidents) aims at feeding incident information back to the entire sector to improve availability nationwide. The project ends in 2019 and hence, no information is available at the time of writing.

The AT is working in co-operation with the Ministry of Economic Affairs and Climate Policy (Economische Zaken en Klimaat, or EZK) and some service providers to investigate whether better quantifiable controls can be used, in order to fulfil the obligation to implement “appropriate measures”. EZK is leading this co-operation from a policy perspective. The European Union Agency for Network and Information Security (ENISA) library of good practices is used as a baseline. The co-operation so far has not resulted in better quantifiable controls or defined standard and target values, but all stakeholders participating are willing to improve monitoring and governance of the telecommunications infrastructure. It has to be noted that participation on this project is not obligatory for all telecommunication providers. Also, agreement has been reached about reporting incidents involving outages for customers (above a certain threshold). Serious incidents always have to be reported, and with this agreement also less serious incidents are reported. The purpose is to evaluate these incidents and see if continuity aspects can be improved.

In practice, the AT only audits companies which have been registered with the ACM as operators of telecommunications infrastructure, including virtual network operators The AMS-IX for example is not registered with the ACM, as it is not subjected to the Dutch Telecommunication Law. However, it is the biggest internet exchange in the world and is subject to the EU Network and Information Security directive regulations. Regular audits of the AMS-IX are not performed by the AT. From a governing perspective, this is not a balanced situation.

Operators have to share information with AT. The AT is subject to public disclosure requests. The law on public disclosure has some provisions to ensure that information which has been shared in confidence by operators will not be shared. A public disclosure request with regard to the Diemen 2017 power outage has shown that the government adheres to the provisions in the law [EZK171]. In order to protect both private and public interests, it is important that the proposed new law on public disclosure will have the same provisions [Dut16].

AT expects a shift in market regulation whereby telephony and SMS services are less important than internet services, with a possible exception of the 112 service. Cyber security related incidents are only incidentally reported to AT, due to the fact that they don’t normally cause continuity problems, which are ground for formal reporting. Hence, AT does not have any indication whether cyber security related issues are rising. It has to be noted that the regulatory body for cyber security (as part of the Dutch NIS implementation) is the NCSC, which is part of the Justice & Security department. From an AT point of view, the importance of telecommunication services is getting more critical and hence, proper governmental oversight will continue to be needed. The power outages which occurred in the last couple of years have showed that outage repair times could have been reduced, in case of operational mobile services.

From an availability perspective, AT aims at improving the relationship between power grid operators, telecommunication service providers and the Safety Regions (Veiligheidsregio’s). The Safety regions already plan table-top exercises whereby telecommunication providers and power grid operators are involved, but in real crisis situations, communication issues are still present.

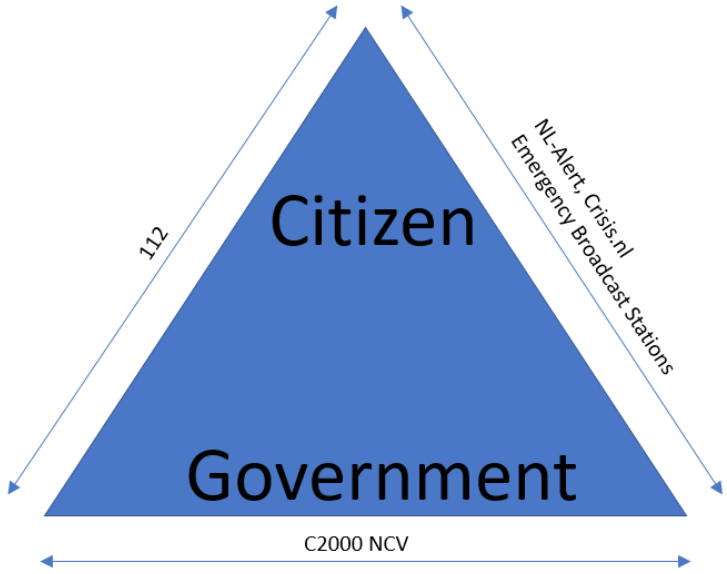

Figure 4 Communication Triangle [Ins15]

AT also expects that WhatsApp and Facebook will play a bigger role in future communication. These OTT-services are missing in the communication triangle (Figure 4), which has been published as part of the report about the power outage of 2015 [Ins15]. AT informed us that ENISA discusses continuity issues with the OTT players as part of the preparations for the European Electronic Communications Code [Eur163]. The discussions concern not only availability, but also integrity and authenticity of communication services. AT has asked for expansion of article 3 of the Radio Equipment Directive [Eur142], to ensure that Internet-of-Things devices will comply with cyber security requirements. AT expects that when this law becomes effective, more regulation effort is required, due to the increased amount of parties which are subject to regulation and audits.

In order to reach out to society, AT has started the program Telekwetsbaarheid[Pro17] as mentioned in chapter 4. When people are aware of risk, they may act and take preparations to ensure that outages don't have a big impact.

AT has co-operated with the EZK department to have continuity requirements added to the auction for mobile frequencies in 2019. The EZK department has written a consultation report for this auction in which also continuity aspects are mentioned. EZK intends to add requirements stating that mobile coverage must be at least 98% per municipality [EZK17]. The report also states that mobile communication is a need and that availability is very important, whereby it is stated that some operators use battery back-up on mobile base station locations to counteract short power outages. The report also discusses specific mobile requirements for the public security and safety sector. Details are stated in an appendix of the EZK report [Str17]. Recommendations are aimed at governments and public security and safety sector institutions. The report gives some interesting scenarios, including a specific government operator using the 700 MHz bandwidth to provide security and safety organisations with reliable telecommunication services. A very interesting conclusion is that the security and safety institutions must set availability requirements first.

7.2 Government as Policy Maker

The Department EZK, is the department responsible for economic progress, anti-trust and competition in economical markets, the environment and continuity and security of critical telecommunication and energy infrastructure in the Netherlands. The Ministry of Justitie & Veiligheid (J&V, Justice and Security) is responsible for the police forces, law enforcement and the judicial system. The J&V department also

manages the National Cyber Security Centre. For this thesis, the chairman of the NCO-T (Nationaal Continuïteitsoverleg-Telecom, National Continuity Council Telecom) has been interviewed.

Based on the interview, EZK considers availability of telecommunication services in the Netherlands very high, and apparently the "*right things*" are done. What is the main factor of success with regard to this availability is not known, and it is expected that a multitude of factors all attribute to the level of availability, whereby providers can take the biggest credit.

Not all providers are aiming for the same level of continuity and security. Within the sector, there are also operators with differently focused business models aiming at other segments of the telecommunication market. Now, there is a standard approach with regard to governance. It might be worth considering a more risk based approach towards governance. A risk based approach is already used for contractors performing underground cable and pipe laying and repair work. Contractors damaging underground infrastructure can be put on a black list [Kad17]. The baseline in this approach is that competition within the market works and that worst players will be forced to act by market pressure first, followed by government pressure when necessary.

EZK also sees the inevitable move from traditional telecommunication as an additional service to an all-over present and needed piece of infrastructure. The novel "*Blackout*" mentions the risk that production can be affected by smart meters or solar panel yards being hacked[Els12]. Current regulation still has focus on the large players in telecommunication and IT infrastructure, covered by Telecommunication law and NIS, but all the small players which are not known may have an impact on critical infrastructure as well, as the DigiNotar incident did show in 2011. System thinking and scenario thinking is critical to work out these scenarios, and the various departments of the government must work together to ensure that appropriate controls are in place.

The rapid growth of Internet of Things (IoT) has forced EZK to think about possible regulation. The new Dutch government coalition wants to establish a roadmap with measures to prevent disasters [VVD17]. These measures do not necessarily mean implementation of new laws and regulation. Externality of risk is seen as a fundamental issue with IoT: Suppliers of IoT devices will in general not feel the need to improve security and most consumers don't ask for security. Hence, the new coalition desires regulation in place to prevent incidents, due to IoT security issues.

EZK has their minds clearly set on the future with regard to regulation and policy making. Given the dependency on telecommunication services, how would society be able to cope with a weeklong outage of power and communication services? Do people have cash, food and drinks and other necessities at home to survive for a week? Grocery stores use Just-in-time ordering and delivery of goods and cash is almost replaced with debit card transactions. Are shops and companies able to sustain their businesses without power and/or telecommunication? These are all questions which are part of the wicked problem of continuity for Dutch society.

From an EZK perspective, it is hard to define actual quantifiable numbers: What is acceptable with regard to loss of service? How fast must recovery be possible? How many people may be affected. How to defend these selected availability figures as a politician, if it goes wrong? People seem to expect to live in a risk-less society. Quantifiable requirements on continuity may make it easier to fine companies which can't reach the goals, but would it really help to improve continuity or is it better to promote and nudge awareness, information sharing and personal responsibility to obtain the desired results?

The current open law, which states that appropriate controls must be taken is a firm basis according to EZK, whereby attention to processes and communication is important. From an EZK perspective, knowledge about technology used is useful to make policies, however, laws and regulation must be agnostic. Technology advances so rapidly that it is assumed that operators already have to work hard to keep up with all the changes in technology.

The telecommunication providers feel the need for extra guidance with regard to these appropriate controls and are co-operating with EZK in the NCO-T to work on clearer definitions which can be used. These discussions are based upon ENISA best practices and recommendations, given the fact that ENISA is a European institution. The discussions have not been finalised and co-operation is on a voluntary basis without any restrictions. This principle is deliberately chosen in order to minimise the legal pressure for participating providers. A provider who does not want to participate in the NCO-T discussions, will still have to adhere to the open norms specified. A draft document is already available, but it is not available for this research. The focus of the document is on processes. At the moment of writing, there is no feedback planned towards ENISA.

EZK also had research performed by the Dutch Normalisation Institute NEN, whether guidance on the open norms could be defined[AGC15][5]. This research proved difficult, due to the fact that there was a focus on solutions, rather than on underlying problems. From EZK perspective, it is necessary to use scenario thinking, whereby probable problems are defined. Based on these defined problems, criteria can be formulated which lead to possible solutions, instead of the other way round. These solutions must work to correct problems, but preferably also to prevent problems.

Determining how much more battery capacity is needed is considered a delicate issue given the goals and perspectives of the range of stakeholders and requires a broader discussion within Dutch society. Consumers want cheap services, but will complain about continuity if they are personally affected. Services such as 112 and C2000 must always be available (Private providers deliver part of the network infrastructure, the government runs the operations. Recent information is not available, but the Antennebureau website of EZK states a minimum availability of C2000 of 98%[Ant13]) and in case of power outages, communication is still key to solve the causes of the outage and to protect citizens and businesses in the affected area. Both within government and in the private sector, money is always an issue and the cheapest bidder on a contract might quite often have a big advantage. This is partially caused by the generic high availability of services, making continuity a less important topic.

The dependency between the various critical infrastructure sectors is a cause for concern according to EZK. Information sharing between sectors has proven not to be so easy, both for preventive and reactive situations. It is felt that inter-sector information sharing can be improved.

EZK aims for a society wide discussion about continuity of services and the price to pay for availability of these services. Are the telecommunication providers the primary party to invest (or shall electricity companies pay the bill), whereby eventually the consumers will pay the price, through raised network subscription fees), or do we accept a certain level of unavailability as society? In that last scenario, everyone can take his/her own responsibility and take appropriate measures to his/her own risk appetite.

From a security point of view, EZK has followed the discussions between Chinese suppliers and the American government in 2012 closely, which were mentioned in the 2012 House of Representatives report[Rog12]. EZK has discussed this topic within the NCO-T. It is outside the scope of this thesis to discuss details about this issue. This is however a responsibility of the providers and it cannot be reasonably expected that all previously installed suspicious equipment can be removed without major investments in new equipment, of which integrity can also not be guaranteed. From a generic point of view EZK maintains the view that it is better for providers not to trust any provider or country, as was shown clearly in the hack of Belgian provider Belgacom by the British secret service GCHQ [Gal14]. Providers are expected to show due diligence and implement appropriate controls to counteract this threat.

The take-over attempt of KPN and the public and political responses can be seen as renewed attention for public interests and national safety and security, after years of privatisation, liberalisation etc. From an EZK perspective, it is important to keep economic trends in balance with security requirements for society.

5 Direct references could not be found by the author of this thesis

Shareholder interests are important, but society interests with regard to critical infrastructure cannot be neglected. Hence from a political point of view, governance efforts are necessary to continuously improve safety, security and continuity for society.

7.3 Politicians

Even though the authors have not been able to have an interview with a politician, a couple of observations have been made based on the interviews. At all the interviews, the topic of how politicians act and respond was mentioned by all of the people interviewed.

Politicians appear to society to be responding too much on incidents without paying attention to a more strategic level of law making. This society which is driven by an overload of news, opinions and calls for action are seen as major drivers, steering this behaviour. There is however a big difference between members of the EU parliament and members of Dutch parliament. The EU members don't feel the pressure of society as the national members of parliament do and hence, don't feel the need to respond to all kind of daily events and issues. Interviewees held the opinion that EU members of parliament have more attention to strategic issues and help nations by providing laws and legal frameworks for issues to come. The national members of parliament, which are working under constant pressure of media and society, must quite often act in order to calm down society even though most issues would solve itself in the long run without political interference. The use of 'symboolpolitiek' (Gesture politics, A Dutch term describing a law which has minor consequences but can be used as a short-term control), is seen as a valid way to deal with certain kinds of social unrest and help to keep the peace, by giving policy makers time to work out structural solutions.

In order to help politicians, reporting is paramount, to ensure that politicians and ministers do possess correct and detailed information about all relevant topics. Better communication and protection against public disclosure of commercial information given by telecommunication providers would also help politicians to get a better understanding of issues within the critical infrastructure, and at the same time better tools to respond. From a politician's perspective, not acting upon incidents is not an option. A politician will be more assured when he/she can inform society that incidents have happened, that the consequences are already minimized by preventive actions, and hence actions have already been taken.

7.4 Telecommunication Service providers

From a provider's perspective, employees from two telecommunication service providers have been interviewed. The author of this thesis has spoken with employees from Vodafone/Ziggo and with employees from KPN. Both companies provide a wide range of fixed and mobile telecommunication services and also deliver services to the Dutch government. The text of the interviews has been bundled to give a complete overview. Both companies have quite similar views with regard to critical telecommunication infrastructure.

Both providers are involved in a lot of discussions with AT and EZK about appropriate controls and directives by the minister, whereby the NCO-T is an important communication channel. Within the NCO-T, involved parties are co-operating on a voluntary basis to define appropriate controls to ensure availability of critical telecommunication services. Both operators interviewed share the opinion that better defined controls are desired. Focus is on continuity plans, crisis teams and communications.

Even though the communication within the NCO-T is good, operators want to have a better communication with other sectors of the critical infrastructure and better communication in case of crisis and outages to improve resilience. Critical infrastructure providers should have the obligation to inform each other in outage situations, so all parties can act faster and more effective to restore functionality. Due to the fact that both electricity networks and telecommunication networks are governed from the DGET (Directorate General Electricity, Telecommunications and competitive markets), it is suggested to have the EZK Department Crisis Organisation involved in crisis mitigation.

With regard to appropriate controls, it is felt that battery back-up of mobile base stations is the most urgent topic to deal with. Fixed network access for consumers and businesses is considered useless by both operators for an area as soon as power outages hit that area. The main cause for this is the fact that customer premises equipment needs power, with the exception of analogue telephone equipment. The point of view from telecommunication service providers is that, even though it is possible to expand the battery capacity, investment by the telecommunication companies would be an externalization for the electricity distribution companies. These companies have the obligation to deliver electricity and also need the telecommunication infrastructure to shorten the restoration timeframes.

Providers want to have a discussion within society about expanding battery capacity for base stations. Providers can pay the bill and will have to make the consumers pay for the higher installation and maintenance costs of the expanded battery capacity. The underlying question is whether customers want to pay extra for a small increase in availability or that it is better to aim for more awareness and maintain the service as is. Investments to increase availability are not linear, the last tenth of percent's of availability will require high investments. Both operators mention that even corporate organisations do not want to pay for high availability solutions due to the fact that regular availability is already very high.

It has been mentioned that the English regulator Ofcom has provided broadband providers with guidelines to supply modems which have a back-up battery functionality. Consumers can use the battery functionality when it is desired. It is the responsibility of the consumer to use batteries and not of the operators[Ofc11].

With regard to the ministerial directives as set in Telecommunication law, article 14, the providers do not know what and how to expect. It is assumed that directives will be used to ensure capacity for critical government services, blocking services or access to services or to help the government with technical means. These probable directives are however assumptions and providers have requested EZK to provide possible directives based on scenarios, to ensure that providers can anticipate on these directives and prepare their organisations. This will act as a double-edged sword, whereby providers know what to expect and governments can rely on results being delivered faster than it would be in case providers have to start acting after a directive has been issued in time of crisis.

The NL-Alert service is seen by operators as a telecommunication law article 14 ministerial directive, due to the fact that all mobile operators had to implement this service. The regional roaming initiative is seen as a voluntary service provided by Vodafone, KPN and T-Mobile. Tele2 is not participating in this service at the moment of writing.

Operators value their internet access services as class A critical infrastructure, given the digitization of Dutch society. Without IT and telecommunication facilities, there are no parts of Dutch society which can still function.

The most important service considered by operators is the 112 service. Both the operators and AT use call generators to ensure that the level of service can be maintained and that interruptions are detected as soon as possible.

The government is considered not to be very consistent in regulation by both operators. The new law on intelligence services [Rij17] was supposed to have requirements on operators to share digital keys. These kinds of requirements undermine security of digital encryption and signing. Operators have objected against this proposal, to ensure availability and integrity of services. Other examples are regulation with regard to net neutrality and deep packet inspection. Operators realize that these technologies can be abused in order to make more profit, but these techniques can also be used to detect and fight malware and cybercrime. Further research into this field is recommended by operators.

From an operator perspective, the AT oversight is considered good, even though the supporting laws and regulations don't help to give clear indications of what is supposed to be done by operators. It is felt

however that AT has to conform to multiple governmental departments, i.e. J&V and EZK and that different governmental business cultures make co-operation and communication hard.

7.5 Consumers of critical telecommunication infrastructure

Interviews have been conducted with an owner of a smaller business and with an IT-architect of an insurance company. The interview with the smaller business owner has been conducted shortly after the Apache power outage incident. The owner of this business is active on Facebook with a local page about Culemborg news. Culemborg is one of the areas which has been affected by the power outage. Based on this interview and some other more informal discussions with company owners, more insights have been gained on the motivations and assumptions of people with regard to critical telecommunications infrastructure.

Both the business owner and the IT architect acknowledge the fact that cloudification is a major change. On premises servers and networks are getting less important and cloud services become more important. Flexibility, time-to-market and pricing are the drivers for this trend. Availability and back-up requirements are made for cloud based services according to both persons interviewed. From a continuity awareness perspective, this is a good sign, although it must not be taken for granted that every business will have taken such controls into account. Cloudification in itself is still an area of concern. Cloud providers can be Dutch providers, but also bigger companies such as Microsoft and Amazon. Where the servers will be located is not transparent to the consumers of these cloud services, but will often be determined by the cloud providers.

A new problem hence, is accessibility to the cloud services used. In case of on-premise servers and applications, companies are more in control of continuity. Equipment such as uninterruptable power supplies can be used to continue production in case of power outages. Companies can decide whether to invest in these kind of solutions or not. In case of cloud based services, power outages can cause loss of connectivity and render the on-premise equipment of a company useless for the duration of an outage.

Both persons interviewed also worried about the continuously increasing impact of telecommunications on society. These concerns are also felt by the other persons interviewed for this thesis. How can providers continue to protect networks and technology and ensure that consumers can use these products in a secure way with a high availability? From a consumer point of view, risk is unknown and hard to grasp, even though from a continuity perspective, the availability of the telecommunications infrastructure is seen as very high by both persons interviewed.

7.6 Interview with a telecommunication scholar

In order to verify some of the conclusion about the laws and regulation, Paul Knol, one of the authors of the Telecommunication law books [Kno15] was interviewed. Paul also works at KPN as a lawyer and extra care has been taken to ensure that this interview was influenced by a KPN bias from my perspective.

Telecommunication law is seen by Mr. Knol as an immature part of the European and Dutch legal system, whereby reporting of incidents and auditing of processes are the focal points for enforcement of law. Modern mature laws sets quantifiable norms. For telecommunication, there are still too many issues with regard to development of services and changes in what is considered relevant. The European institutes ENISA and ETSI are running projects to increase maturity by adding quantifiable controls, but when part of these controls can be implemented is not known.

The NIS is welcomed by Mr. Knol due to the fact that not only the traditional telecommunication providers are regulated, but that also other critical IT suppliers, such as certificate providers and internet exchanges are part of regulation. The EECC does exist since 2002, has been revised in 2009 and is currently being redesigned to include over-the-top players as well. This is seen as a breakthrough, but it has to be seen how OTT players will be enforced to comply with the law: How are foreign players, which have their servers located in other continents, being forced to comply with the law, even though they have millions

of users and play a big role in crisis communication? Continuity of the services OTT players deliver depends on multiple aspects out of reach and influence for European law.

Given the role of OTT players in communication and their business model, more research is needed on how to regulate these companies and how to use their services from a government perspective. If the governmental agencies using the services, then these agencies are not customers, but are also part of the product of these companies. Based on all the communication of users on these networks, these OTT players will have a better picture of the impact of issues happening in society than local companies and the Dutch government will have.

Due to the telecommunication landscape getting more complex and gaining importance due to trends such as IoT, autonomous vehicles etc, political governance is a wicked problem. A wicked problem is a problem with no strictly definable description, involves many stakeholders, has no single and simple solutions which can solve the problem [Rit73]. Added to these governance issues is a society which is less willing to accept risk, leaving politicians will less options to act. Gesture acts might be a solution to temporarily solve some easier issues.

The take-over attempt of KPN has kept both KPN lawyers as well as EZK lawyers busy for a while. The current Dutch laws did not provide enough legal provisions to block the take-over. A private sector institution managed to block the attempt, but this is not possible for every private company because not every company has these protection mechanisms defined. An interesting point of view is whether a take-over by another foreign telecommunication company would be a bad situation for the security and continuity of critical infrastructure. A telecommunication company has to provide customers with the best products and knows how the telecommunication market functions, even on a detailed level. A take-over by a hedge-fund would have been worse, due to the interests of the hedge fund being non-aligned with the continuity interests of the telecommunications company and society.

An item quite overlooked is the fact that critical telecommunications operators might have outsourced parts of network management. This results in operators having less knowledge about detailed parts of network design and should lead to outsource contractors having to confirm to applicable laws such as Telecommunication law and NIS. As an example given during the interview, the fire in the broadcast tower of Smilde in 2011 was not a KPN responsibility and the company owning the towers was not well-known from a law and regulation principle. An interesting aspect with regard to outsourcing are the requirements set by the government for clearance of employees working with critical infrastructure, including the guidelines as set by the AIVD intelligence service [AIV14].

From a fundamental point of view, should the government have a big influence on the telecommunications market? Mister Knol argues that competition in the market should be the determining factor. It was a government decision to privatise KPN and hence, government influence on KPN must be reduced. From a market perspective the government does not have the technical knowledge to really improve continuity. How can an auditing organisation verify whether the right moves are made by a telecommunications company to increase robustness and reliability of its infrastructure?

From a governmental perspective, actions should be more rational, due to the financial impact on society and companies involved. For example with mobile coverage, politicians can be persuaded to promote 100% coverage, even though this can become expensive and hard to arrange. There have been situations whereby people complain about lack of coverage, but at the same time block attempts to have a mobile base station installed due to fears of radiation or fears of the landscape being spoiled by a high antennae.

8 Drawing Conclusions, defining weaknesses and improvement opportunities.

This thesis has been written as part of a master's study in cyber security. The subject matter chosen is a subject close at heart of me. Security of society is an important topic and telecommunication networks play an important role in this perspective. Due to the fact that I work for one of the Dutch telecommunication providers, I have taken this bias into consideration in every phase and step of the research. Information mentioned in this thesis is all based on information which is publicly available, or based on interview information which could be openly shared. The amount of publicly available information about telecommunication infrastructure is scarce compared with what I know about this topic. Writing the thesis has been a matter of using restraint.

Based on the literature study and the interviews, both strong and weak points of law and regulation have been found. Based on the research questions, the strength and weaknesses are summarised:

Are the Dutch government controls for the protection of critical telecommunications infrastructure sufficient and effective?

Combining both the literature study and the interviews, the answer is a moderate yes. Dutch critical telecommunication infrastructure availability is one of the highest in the world. The applicable Dutch laws and regulations are very much in line with European laws and regulation. Based on both desk research and interviews, it has not been possible to find evidence to state that laws and regulations are the main driving force in, keeping the availability of infrastructure at the current level. The telecommunication service providers play an important role in keeping the infrastructure available as they are responsible for the reliable design and operations of their networks. Whether the laws and regulations are sufficient and effective in protecting the critical telecommunications infrastructure is difficult to judge based on the literature study. The definition of both terms as given in paragraph 4.1 can lead to multiple interpretations. What is sufficient or effective for the government as lawmaker can differs from the perspective of government as a regulator. Given the fact that Dutch infrastructure in general ranks 5th worldwide and the fact that regulation for critical infrastructure has many common aspects for all sectors, the controls are sufficient. The needs (high availability) of the situation (the Dutch telecommunication infrastructure) are met. The people interviewed were in general satisfied with the level of sufficiency, but argued that effectiveness could be improved, for example by having reporting obligations centralised instead of the current fragmented situation. According to the definitions cited, controls are effective if the desired effect is reached, or when a control is decisive. Based on the Dutch quality ranking, the controls are effective. Due to the fact that the controls are qualitative in nature and lack quantitatively measurable settings, the interviews show some reservations in regard to the definition of effectiveness. This conclusion reflects the thoughts and suggestions with regard to improvements of effectiveness.

Of the people interviewed, no-one could point out a single factor of success and hence it is assumed that other factors such as awareness within the sector, geographical situation, infrastructure architecture, competition, and market demands contribute to the continuity aspects. I have focused on the other research questions to determine if I could determine whether the current high level of continuity could be improved or at least kept at the same level. The main research question which is asked in the thesis is:

- *Which legal controls can the government implement to gain greater control, by adapting laws and regulations, of privately owned critical telecommunications infrastructure given the threats the Dutch society is facing?*

The laws and regulations in place are qualitative in nature, describing processes and documentation, rather than specific availability requirements, such as a monthly or annual availability percentages and restoration timeframes during incidents. I understand that these numbers are difficult to define and somewhat debatable, especially in the aftermath of an incident. Members of the cabinet must be able to

defend these statistics in parliament. However, when governmental departments are In need of critical telecommunication services, it is recommended to define criteria, so the critical telecommunication infrastructure providers can offer their services based on the requirements as set by the governmental departments. This recommendation was also published in the report by Stratix about 700Mhz broadband communications. The fact that multiple stakeholders all agree on having clearer metrics, must be a driver to proceed with efforts to reach agreement on the use of quantifiable metrics.

In addition or as an alternative, the government can choose to use a comparative standard. The current ranking of the Netherlands as 5th on a global level and 1st as an European Union member can be set as a target which must continue to be met by the operators of critical Dutch infrastructure. The government must in that case ensure that there are insights into how this ranking is determined and which factors discriminate the various sectors. When a ranking falls, the cause must be able to be pin-pointed, otherwise counteracting the fall in ranking is not possible.

In order to understand the laws and regulations, their influences and limitations, the following questions have been elaborated upon:

- *Who are the main stakeholders involved?*
    - *What are their needs and drivers?*

In order to understand how laws and regulations effect the critical infrastructure, the systems theory was used to compose a model of the critical telecommunications infrastructure landscape based on a regulatory model. In this model, the laws and regulations are dominated by the European Union lawmakers. Given the fact that telecommunications infrastructure is of great importance to economic development, the European Union has established a variety of laws to protect telecommunications infrastructure and ensure a level playing field for all involved parties. The previous laws and regulations dealt with traditional telecommunications companies, which were expanded to other European IT sectors over time delivering parts of critical infrastructure. The upcoming law puts the Over-the-top players under the influence of the law too.

The Dutch government has put laws and regulation into effect for the telecommunications sector and also enforces European directives such as the NIS (Operator of Essential Services). The departments of Justice & Security (J&V) and Economical Affairs & Climate Policy (EZK) are responsible for respectively security and continuity of the critical telecommunication sector. For both critical IT and critical telecommunications, there are departmental offices to report incidents to. The J&V department has the NCSC, which can help companies and institutions with IT related security issues and to which incidents must be reported. The EZK department has the AT office for all critical telecommunications related governance. The J&V drivers are national security and law enforcement. The EZK department has a variety of drivers from ensuring an open and competitive telecommunications market to the continuity of critical infrastructure in the Netherlands. This last driver is shared with the J&V department. The crisis management structure of the Dutch government is very thorough in setup and nature. Private-public partnership is a key issue in crisis management and is given substantial attention in policy documents.

The companies regulated by the telecommunication law nowadays (and in the near future by the NIS regulation) are companies which operate in the critical telecommunications infrastructure such as the traditional telephony operators (which all expanded their business to include other critical services such as internet access), Internet exchanges such as the AMS-IX, certificate providers and other players. From a regulatory point of view, focus is still on the critical telecommunications providers, due to the fact that connectivity to services is important for all other sectors and society. These private parties are all commercial and must make profit to stay in business. Competition is fierce in this sector although limited to a small number of companies which own a network. Based on availability figures, these companies have found a balance between economy and security. Other services such as hosting and housing can be provided by smaller companies and these normally do not present a threat to continuity of services.

However, care must be taken not to overlook small but essential companies such as DigiNotar, which caused a world-wide crisis with its digital certificates.

Consumers of the services provided are the other major stakeholder. The government is seen as a stakeholder from a consumer perspective. In general, Dutch stakeholders are used to a high availability level and expect availability to stay on a high level. Awareness of outages is present by consumers and businesses interviewed and studied. However, preventive controls in use by consumers and organisations are differ widely given the diverse risk appetites of consumers and businesses served by the telecommunications sector.

The OTT-players are an interesting stakeholder. Their communication services are used by almost all consumers. The government uses OTT services as primary method of communication. These companies are barely regulated and their business models can be challenging to understand. In the section 8.1, some follow-up research suggestions are given

- *What are the strengths and weaknesses of current critical telecommunication infrastructure related laws and regulations in the Netherlands?*

Based on both desk research and interviews, it can be concluded that current laws and regulation offer a generous field for providers to operate in. Architectural and operational aspects of telecommunication infrastructure are not regulated, hence telecommunication companies can design and operate their own business model as long as availability is delivered.

There is a new law in development to curb foreign influence on critical infrastructure. This law does not appear to take the use of third parties to manage parts of the Dutch critical infrastructure into account. It is suggested that more restraints are introduced to manage these third parties.

The current laws and regulations are qualitative in nature. Furthermore no quantitative norms are in place. This is due to the fact that laws regarding telecommunication are relatively young and still being developed according to the demand from society. Even though it will be difficult to formulate quantitative requirements for uptime and maximum tolerable periods of downtime, defining these numbers for new and existing services should help operators of telecommunication infrastructure create an architectures suitable for future needs. On the other hand, to have standard fixed quantifiable norms implies these must be applied to the entire critical infrastructure sector. The externalisation of costs to improve the robustness mentioned in the analysis may cause issues in the chain of electricity distribution provider to telecommunication provider to consumer. By setting norms solely for the telecommunication sector which will require investment by the telecommunications service providers will almost certainly ensure a price increase for the consumer as a return on investment is expected by the provider. Following on from this theory, the electricity distribution providers should also have a role in fulfilling the burden of the investment. This will in turn reduce the burden for the telecommunication providers. It is however unlikely that consumers would benefit as they will be charged for the services as a total.

The DigiNotar case has shown that fundamental issues exist with regard to the architecture of public key infrastructure by Schneier and Ellison. It is recommended to promote research to find solutions for these issues.

The weakest link in law and regulation seems to be the lack of integration between the various sectors of critical infrastructure. Each sector is regulated without structurally taking other relevant sectors into account. Externalisation of problems is an issue which worries multiple stakeholders. A question often asked is whether the telecommunications companies have to invest to fix a consumer problem caused by the electricity supply? The costs of the investment will eventually be indirectly paid by consumers. Continuity topics are not easy to address in politics, according to the research, multiple parties stated that risk appetite in society is decreasing and politicians are required to approach problems from a technical

point of view. It must however be kept in mind that a lower accepted risk means higher taxes and cost of living. that the general view is that awareness should be raised by consumers to make clear that even though the availability of critical telecommunication infrastructure is high, people and businesses can make their own choices with regard to back-up plans and controls. In short, the availability of critical telecommunications infrastructure is high in The Netherlands and work needs to be done to achieve a similar level of robustness within society.

- *What are the limitations and restraints which must be taken into account by new laws and regulations in the Netherlands?*

Based on the interviews, it can be concluded that more insight in the technical architecture of critical telecommunications providers networks is desired from a governing perspective. A more open communication (given the ability to minimise the effects of public disclosure law on company sensitive information) would help the governing institutions to improve continuity.
There is a delicate balance between anti-trust regulation and continuity. According to an ACM/ Opta/ AT report, telecommunication providers cannot share their infrastructure other than the mobile base stations masts. Co-operation from a continuity perspective could lead to possible competition law suits, despite the primary goal of co-operation being increased continuity.

It is suggested to use less restraint when raising awareness in society. Continuity comes at a price, but society must be aware of this. When society is a suitably prepared, it could be willing to accept higher risks and may take measures at an individual level. The AT awareness campaign is a good start, but needs more media exposure.

- *What are the expected changes and developments impacting the Dutch Telecommunications sector within the next 5 years? Which adaptations on applicable laws and regulations will be required?*

The telecommunication market is a dynamic market. It has not been researched if a different strategy with regard to network operations would work, whereby all operations are undertaken by one operator, as has happened in the electricity and gas sectors.
The outsourcing of network operations by these companies gives cause for concern and it is recommended to carry out further research in this area.
It has been mentioned in the thesis that the importance and dependency of critical telecommunication infrastructure will increase with the rise of IoT, self-driving cars and other new technologies. Society's dependency on electricity will increase. This automatically implies that the government must ensure the continuity of services and therefore for adapt appropriate laws and regulations. Even though it is expected that electricity production will become more local, the speed of that transition will lag behind the trends in communication. The following question has addressed this topic:

- *In which ways can CII (Critical Information Infrastructure) related policies be adapted to suit future needs of Dutch society?*

The current laws focus on the traditional telecommunications sector, whilst society and government already use over-the-top services for official communication purposes and in times of crisis, use OTT communication services as a primary means of communications. New laws and regulations must take the use of OTT services into account.
A better quantification of availability figures, including communication of these figures, will help society to accept the fact that critical infrastructure can fail and that certain services may not always be available.

Based on the interviews, it became apparent that co-operation and communication between the various critical infrastructure sectors can be improved. Within a sector, stakeholders know how to find each other. During an incident, however, impacted stakeholders have to cope with a lack of information, resulting in a slower restoration of services. Reporting and communication during incidents and following up of incidents can all be improved.

- Even though incidents must be reported, this reporting is fragmented over a variety of governmental organisations, such as but not limited to AT and NCSC. The reporting structure is such that it allows the level of public reporting to be harnessed depending on the nature of the company. Open communication between stakeholders is important in order to improve developments in the sector. Public disclosure laws applicable to governmental stakeholders can hamper exchange of information. Laws must ensure that company sensitive information shared, remains confidential. The new law on public disclosure will have an effect on private-public co-operation of which consequences are not yet clear[Dut16]
- When incidents occur, the telecommunication service providers feel that not all information is adequately shared. A common platform operated by NCC, NCSC and used for incident communication could help operators during power outages, for example. The companies involved could publish information about expected restoration times, making it easier for the other providers to decide whether to use alternative means to counteract the outage. Of course, this platform must have the capability to ensure a high availability to enable communication in times of crisis.
- Categorisation of critical communication services needs attention. Together with electricity, internet access and services are at the bottom of the critical services chain and cascading effects can be disastrous. It is suggested that the internet access services are categorised as a Category A critical infrastructure.
- The British Ofcom modem regulation is worth investigation. This regulation enables back-up power functionality whereby the burden is split between operators and customers who have the responsibility of keeping a supply of batteries to power modems during power outages.

8.1 Suggestions for further research

This thesis has shown that laws and regulation help society with the continuity of telecommunication services in The Netherlands. It could not be determined how great the contribution of these laws and regulations is in comparison to factors such as economical drivers and co-operation between parties.

Using a literature study it has been determined that there are sufficient legal frameworks in place at international and Dutch levels. The government has proper mechanisms in place to counter the effects of crisis. Telecommunication companies deliver high available services and it is has been assessed that a suitable overview is in place. Using systems theory the sector has been researched and relationships with society established.

Based on actual cases, the essence for society was sketched and preliminary conclusions drawn. These conclusions were verified and validated using interviews with key stakeholders in the sector. On the basis of the preliminary conclusions in combination with the interviews, the final conclusions are summed up and suggestions for improvement are outlined.

- As mentioned in the conclusions, over-the-top services are used extensively by the government as communication channels. It is unclear how and why all the various governmental departments use these services. Are they a paying consumer or should they be seen as a product of the OTT suppliers What kind of information is collected by these suppliers and who can obtain this information? From a security and economic perspective it is recommended to perform a further study to determine what the impact is of using these services on security and continuity of society.
- Further research is suggested in the areas of how third parties are used in the critical infrastructure sector to manage critical infrastructure and whether extra controls are necessary to prevent crisis situations.
- Further research is also suggested with regard to changing operating models whereby one single operator is responsible for design and operations of the core telecommunication networks, comparable to that of the electricity sector.
- Do penalties help to change behaviour? Should this mechanism be used sparsely? During discussions this topic was touched on , but given my own bias, I refrained from further research on this topic.

9 Bibliography

ACM. (2017, 12 17). *Fusie van CA, NMa en OPTA per 1 Januari 2013 voorzien.* Retrieved from ACM: https://www.acm.nl/nl/publicaties/publicatie/7469/Fusie-van-CA-NMa-en-OPTA-per-1-januari-2013-voorzien

ACM. (2017, 12 18). *Telecomaanbieders, Registratie van Telecomaanbieders*. Retrieved from ACM.nl: https://www.acm.nl/nl/onderwerpen/telecommunicatie/de-telecommarkt/registratie

AG Connect. (2001, 04 19). *Grote telefoonstoring door softwareprobleem*. Retrieved from AG Connect: https://www.agconnect.nl/artikel/grote-telefoonstoring-door-softwareprobleem

AG Connect. (2005, 09 16). *Vodafone gunt netwerkonderhoud aan Ericsson*. Retrieved from https://www.agconnect.nl: https://www.agconnect.nl/artikel/vodafone-gunt-netwerkonderhoud-aan-ericsson

AG Connect. (2015, 03 26). *NEN peilt meningen over Telecomwet*. Retrieved from AG Connect: https://www.agconnect.nl/artikel/nen-peilt-meningen-over-telecomwet

AGCOnnect. (1998, 06 04). *OT2000 in drieën gesplitst*. Retrieved from AGCOnnect: https://www.agconnect.nl/artikel/ot2000-in-drieen-gesplitst

Agentschap Telecom. (2017, 10 12). *Programma Telekwetsbaarheid*. Retrieved from Agentschap Telecom: https://www.agentschaptelecom.nl/algemeen/over-agentschap-telecom/programma-telekwetsbaarheid

Agentschap Telecom. (2017). *Staat van de Ether 2016.* Groningen: Agentschap Telecom.

Agentschap Telecom. (n.d.). *Minimale eisen continuïteitsplan.* Groningen: Agentschap Telecom.

AIVD. (2014). *Leidraad aanwijzing vertrouwensfuncties, nadere uitwerking van de Wet Veiligheidsonderzoeken.* AIVD.

Allcott, H., & Gentzkow, M. (2017, 06). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*, *31*(2), pp. 211-236. Retrieved 09 25, 2017, from https://web.stanford.edu/~gentzkow/research/fakenews.pdf

Allison, G. (1963). Conceptual Models and the Cuban Missile Crisis. *The American Political Science Review*, 689-718.

Amazon Web Services. (2018, 12 18). *AWS Global Infrastructure*. Retrieved from http://aws.amazon.com: https://aws.amazon.com/about-aws/global-infrastructure/

América Móvil trekt bod KPN in. (2016, 10 13). *NOS*, p. 1. Retrieved 03 13, 2017, from http://nos.nl/artikel/563272-america-movil-trekt-bod-kpn-in.html

AMS-IX. (2016). *AMS-IX historical timeline.* Retrieved from AMS-IX: https://ams-ix.net/about/historical-timeline

ANP. (2012, 09 05). *KPN tekent IT-contract met Tech Mahindra*. Retrieved from https://www.nu.nl: https://www.nu.nl/beurs/2901533/kpn-tekent-it-contract-met-tech-mahindra.html

ANP. (2013, 08 09). *América Móvil doet bod op heel KPN*. Retrieved 06 20, 2017, from http://www.nu.nl: http://www.nu.nl/binnenland/3546326/america-movil-doet-bod-heel-kpn.html

ANP. (2017, 04 12). *Extra bescherming bedrijven onnodig volgens belangenclub beleggers*. (http://www.nu.nl, Editor) Retrieved 04 17, 2017, from http://www.nu.nl/beurs/4614276/extra-bescherming-bedrijven-onnodig-volgens-belangenclub-beleggers.htmeri

Antennebureau. (2013, 06 13). *C2000 netwerk voldoet in 2012 aan gestelde normen*. Retrieved from Antennebureau: https://www.antennebureau.nl/actueel/nieuwsberichten/2013/c2000-netwerk-voldoet-2012-aan-gestelde-normen

Antennebureau. (2017, 09 03). *Antennebureau*. Retrieved from http://www.antenneregister.nl: http://www.antenneregister.nl/

Barth, B. (2016, 10 16). *DDoS attacks delay trains, halt transportation services in Sweden*. Retrieved from https://www.scmagazineuk.com: https://www.scmagazineuk.com/ddos-attacks-delay-trains-halt-transportation-services-in-sweden/article/700325/

Beek, van der, P. (2014, 01 06). *Huawei beheert 4G-netwerk T-Mobile*. Retrieved from https://www.Computable.nl: https://www.computable.nl/artikel/nieuws/outsourcing/4967420/250449/huawei-beheert-4g-netwerk-t-mobile.html

Bertalanffy, v. L. (1968). *General System Theory: Foundations, Development, Applications.* New York.

Bloem, W. (Writer), & Blokzijl, J. (Director). (2012). *Sluizen, gemalen en bruggen slecht beveiligd* [Motion Picture]. Netherlands. Retrieved 07 25, 2017, from http://20jaareenvandaag.eenvandaag.nl/hoogtepunten/39770/sluizen_gemalen_en_bruggen_slecht_beveiligd

Bremmer, D. (2017, 02 02). KPN-baas: overheid mag buitenlandse overname KPN niet blokkeren. *Algemeen Dagblad*, p. 1. Retrieved 02 03, 2017, from http://www.ad.nl/economie/kpn-baas-overheid-mag-buitenlandse-overname-kpn-niet-blokkeren~a59dfe36/

Brown, K. (2006). *Critical Path, A Brief History of Critical Infrastructure Protection in the United States.* Fairfax, Virginia: Spectrum Publishing Group.

Buiren, van, K., Fijnje, J., Rougoor, W., Smits, T., & Kocsis, V. (2016). *Telecommunicatie in Caribish Nederland, quick scan onderzoek naar de ordening van de markt voor Telecom in Caribisch Nederland en de ontwikkelingen daarin sinds de transitie.* Amsterdam: SEO Economisch Onderzoek.

Bulten, C., Jong, de, B., Breukink, E.-J., & Jettinghoff, A. (2017). *Vitale Vennootschappen in veilige handen.* Nijmegen: Onderzoekscentrum Onderneming & Recht, Radboud Universiteit NIjmegen.

C2000. (2018, 09 03). *C2000 Homepage*. Retrieved from C2000: https://www.c2000.nl

Centre for Safety and Security in Smart Societies. (2015, 1 1). *LINC: Learning form Incidents*. Retrieved from Universiteit Twente: https://www.utwente.nl/ctit/research/research_projects/national/nwo/Cyber%20Security/linc.html

CIA/FBI/NSA. (2017). *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution.* Washington: Office of the director of National Intelligence (USA).

C-ITS Platform. (2016). *C-ITS Platform Final Report.* Platform for the Deployment of Cooperative Intelligent Transport Systems in the European Union.

Clinton, W. J. (1998). *Presidential directive 1998, number 63 (PDD 63): Critical Infrastructure Protection Directive.* Washington D.C. Retrieved from http://www.ciao.org

Council of Europe. (2001). *Convention on Cybercrime.* Budapest: Council of Europe.

Covey, S. (1989). *The 7 Habits of Highly Effective People.* Free Press.

Cyber Security Raad. (2017, 09 23). *Cyber Security Raad*. Retrieved from https://www.cybersecurityraad.nl/: https://www.cybersecurityraad.nl/

Datacentrum-Datacenter.nl. (2017, 10 13). *Internet Exchange Points in Nederland*. Retrieved from Datacentrum-Datacenter.nl: http://www.datacentrum-datacenter.nl/internet-exchange-points.html

De Nederlandse Bank. (2017, 11 13). *Missie en Taken*. Retrieved from De Nederlandse Bank: https://www.dnb.nl/over-dnb/index.jsp

DelaRue, S., & Seynaeve, M. (2010). *Oorzaken en gevolgen van de economische crisis, en aanbevelingen naar de toekomst: Een verkenning.* Gent: Universiteit Gent, faculteit economie en bedrijfskunde.

Drion, S. (2017, 04 20). *Telecomsector beschermen prima: maar regel het dan wel goed a.u.b.* Retrieved from http://www.VNO-NCW.nl: https://www.vno-ncw.nl/column/telecomsector-beschermen-prima-maar-regel-het-dan-wel-goed-aub

Dunn, M. (2005). The socio-political dimensions of critical information infrastructure protection (CIIP). *Int. J. Critical Infrastructures, 1*(2/3, 2005).

Dutch Cowboys. (2006, 03 10). *SMS 'veel geld' naar Idols*. Retrieved from Dutch Cowboys: http://www.dutchcowboys.nl/mobile/6473

Dutch Government. (1815, 08 24). *Grondwet voor het Koninkrijk der Nederlanden van 24 Augustus 1815*. The Hague.

Dutch Government. (1993). *Wijizging van de Machtigingswet PTT Nederland NV in verband met de opheffing van de verplichting tot splitsing van PTT Telecom B.V.* The Hague: Ministerie van Verkeer en waterstaat.

Dutch Government. (1996, 04 03). Wet van 3 April 1996, houdende regeling met betrekking tot uitzonderingstoestanden. *Coördinatiewet uitzonderingstoestanden*. The Hague.

Dutch Government. (1996). *Wet Veiligheidsonderzoeken.* The Hague: Dutch Government.

Dutch Government. (1998). *Elektriciteitswet 1998.* The Hague: Dutch Government.

Dutch Government. (1999, 02 17). Wet van 3 April 1996, houdende hernieuwde vaststelling van de Oorlogswet voor Nederland ter aanpassing aan de grondwet en aan de Coördinatiewet uitzonderingstoestanden. *Oorlogswet voor Nederland*. The Hague.

Dutch Government. (1999, 07 15). *Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en de Telecommunicatiewet in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II).* The Hague: Dutch Government. Retrieved from Overheid.nl: https://zoek.officielebekendmakingen.nl/kst-26671-3.html#IDAQYEFB

Dutch Government. (2000). *Gaswet.* The Hague: Dutch Government.

Dutch Government. (2000, 07 06). Wet van 6 Juli 2000, houdende regels inzake de bescherming van persoonsgegevens. *Wet Bescherming Persoonsgegevens*. The Hague.

Dutch Government. (2003, 05 21). Wet van 8 mei 2003 tot aanpassing van Boek 3 en Boek 6 van het Burgerlijk Wetboek, de Telecommunicatiewet en de Wet op de economische delicten inzake elektronische handtekeningen ter uitvoering van richtlijn nr. 1999/93/EG van het Europees Parlement en de. *Wet electronische handtekeningen geldend van 21-05-2003 t/m heden*. The Hague.

Dutch Government. (2006). *Wet op het financieel toezicht.* The Hague: Dutch Government.

Dutch Government. (2007). *Besluit van 19 oktober 2007, houdende algemene regels voor inrichtingen (Besluit algemene regels voor inrichtingen milieubeheer).* The Hague: Dutch Goverment.

Dutch Government. (2007, 12 12). Regeling van de Staatssecretaris van Economische Zaken van 11 december 2007, nr. WJZ 7119637 houdende vaststelling van bepalingen ter zake van de voorbereiding op buitengewone omstandigheden in de sector Telecommunicatie. *Regeling voorbereiding buitengewone omstandigheden sector Telecommunicatie 2007*. The Hague.

Dutch Government. (2008, 07 25). Rijkswet houdende goedkeuring Verdrag van Lissabon tot wijziging van het verdrag en het Verdrag tot oprichting van de Europese Gemeenschap, geldend van 25-07-2008 t/m heden. The Hague.

Dutch Government. (2009). *Drinkwaterwet, geldend van 01-07-2015 t/m heden.* The Hague: Dutch Government.

Dutch Government. (2010, 02 11). Wet van 11 februari 2010, houdende bepalingen over de brandweerzorg, de rampenbestrijding, de crisisbeheersing en de geneeskudige hulpverlening. *Wet Veiligheidsregio's*. The Hague.

Dutch Government. (2012, 10 19). Besluit van 19 oktober 2012, houdende nadere regels met betrekking tot technische en organisatorische eisen ter beperking van risico's voor de veiligheid en de integriteit, de meldplicht van inbreuken op de veiligheid en verliezen van integriteit, de vers. *Besluit continuïteit openbare electronische communicatienetwerken en -diensten, geldend van 01-01-02017 t/m heden*. The Hague.

Dutch Government. (2014, 08 01). Wet van 19 Januari 2012 inzake instelling van de Raad voor de leefomgeving en infrastructuur. *Wet Raad voor de leefomgeving en infrastructuur*. The Hague.

Dutch Government. (2016, 11 14). *Voorstel van wet van de leden Voortman en Van Weyenberg houdende regels over de toegankelijkheid van informatie van publiek belang (Wet open overheid).* The Hague: Eerste Kamer der Staten-Generaak. Retrieved from Eerstekamer: https://www.eerstekamer.nl/wetsvoorstel/33328_initiatiefvoorstel_voortman

Dutch Government. (2017, 07 01). Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie. *Telecommunicatiewet*. The Hague, Netherlands: Dutch Government.

Eerste Kamer der Staten Generaal. (Vergaderjaar 2012-2013). *Verbinding Verbroken: Onderzoek naar de Parlementaire besluitvorming over de privatisering en verzelfstandiging van overheidsdiensten.* The Hague: Eerste Kamer der Staten Generaal.

Eldik, van, G. (2017, 11 15). *Maandagavond. De stroom valt uit...* Retrieved from Facebook: https://www.facebook.com/gerard.van.eldik/posts/10212880783628530

Elsberg, M. (2012). *Blackout – Morgen ist es zu spät.* Black Swan.

ENISA. (2017, 11 09). *European Union Agency for Network and Information Security*. Retrieved from ENISA: https://www.enisa.europa.eu/

ETSI. (2015, 12 15). *European Telecommunication and Standardisation Institute*. Retrieved from ETSI: http://www.etsi.org/

European Union - Directorate General for Communication. (2012). *How the European Union works, Your guide to the EU institutions.* Luxembourg: European Union.

European Union. (2002, 03 07). Directive 2002/21/EC of the European Parliament and of The Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services.

European Union. (2014). *Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.* European Union.

European Union. (2014, 07 23). Regulation (EU) No 910/2014 of the European Parliament and of The Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/EC. *eIDAS regulation*.

European Union. (2014, 03 11). Regulation (EU) No. 283/2014 of the European Parliament and of The Council of 11 March 2014 on guidelines for trans-European networks in the area of telecommunications infrastructure and repealing Decision No 1336/97 EC.

European Union. (2015). *Regulation (eu) 2015/758 of the European Parliament and of the Council of 29 april 2015 concerning type-approval requirements for the deployment of the ecall in-vehicle system based on the 112 service and amending directive 2007/46/ec.* European Union.

European Union. (2016, 06 07). Consolidated version of the Treaty on European Union and the Treaty on the functioning of the European Union. *Treaty on European Union*. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2016:202:FULL&from=EN

European Union. (2016, 07 06). Directive (EU) 2016/1148 of the European Parliament and of the council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Directive on security of network and information systems*.

European Union. (2016). *Directive of the European Union Parliament and of the Council Establishing the European Electronic Communication Code.* Brussels: European Union.

European Union. (2016, 04 27). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. *General Data Protection Regulation*.

EZK DGET. (2006). *Handboek Nationaal Continuïteitsoverleg - Telecommunicatie.* The Hague: Ministerie van Economische Zaken DGET.

EZK DGET. (2008). *Handboek Nationaal Continuïteitsoverleg - Telecommunicatie Bijlagen.* The Hague: Ministerie van Economische Zaken DGET.

EZK DGET. (2017, 06 15). *Besluit op WOB-verzoek met betrekking op de stroomstoring op 17 januari 2017 aan de Hemweg in Amsterdam.* Retrieved from Rijksoverheid.nl: https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/15/besluit-op-wob-verzoek-stroomstoring-hemweg-amsterdam-17-januari

FIRST. (2017, 12 128). *About Forum of Incident Response and Security Teams*. Retrieved from FIRST.org: https://first.org/about/

FIRST. (2017, 12 18). *FIRST members around the world*. Retrieved from FIRST.org: https://first.org/members/map

Foundation Preference Shares KPN. (2013). *Press release Foundation Preference Shares B KPN exercises option.* Amsterdam: Foundation Preference Shares KPN.

Freeman, R. L. (1999). *Fundamentals of Telecommunications.* New York: John Wiley & Sons, Inc.

Fretten, C., & Miller, V. (2005). *The European Union: A Guide to terminology, procedure and sources.* House of Commons Library.

Gallagher, R. (2014, 12 13). *Operation Socialist; The inside story of how British spies hacked Belgium's largest Telco.* Retrieved from The Intercept: https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/

Gelder, de, M. (2016). Het NAFIN transport netwerk, Derde generatie Wide Area Network in het Statische domein. *Intercom*, *2*, p. 7.

GFCE. (2015). *Launch of the Global Forum on Cyber Expertise, The Hague Declaration on the GFCE.* The Hague: Global Forum on Cyber Expertise. Retrieved from https://www.thegfce.com/

Greenemeier, L. (2013, 09 18). *NSA Efforts to Evade Encryption Technology Damaged U.S. Cryptography Standard*. Retrieved from Scientific American: https://www.scientificamerican.com/article/nsa-nist-encryption-scandal/

Grierson, J. (2018, 12 18). *Russia-linked Twitter accounts 'tried to divide UK' after terrorist attacks*. Retrieved from The Guardian: https://www.theguardian.com/uk-news/2017/dec/18/russia-linked-twitter-accounts-tried-to-divide-uk-after-terrorist-attacks

Haes, de, U. (2011, 09 12). *Donner dreigde DigiNotar met nachtelijke rechtszaak.* Retrieved from http://www.webwereld.nl: http://webwereld.nl/security/54707-donner-dreigde-diginotar-met-nachtelijke-rechtszaak

Heemskerk, F. (2007). *Instellingsbesluit Nationaal Continuïteitsoverleg Telecommunicatie 2007.* The Hague: Ministerie van Economische Zaken.

Hollander, de, G., Vonk, M., Snellen, D., & Huitzing, H. (2017). *Mobiliteit en elektriciteit in het digitale tijdperk, Publieke waarden onder spanning*. Planbureau voor de Leefomgeving.

https://www.submarinecablemap.com. (2017). *Submarine cable maps*. Retrieved from https://www.submarinecablemap.com/: https://www.submarinecablemap.com/

Huijbrechts, J. (2017, 03 31). *Ziggo heeft dns-storing - update*. Retrieved from http://www.tweakers.net: https://tweakers.net/nieuws/123017/ziggo-heeft-dns-storing.html

ICANN. (2015). *The IANA functions; An Introduction to the Internet Assigned Numbers Authority (IANA) Functions.* ICANN.

ICANN. (2017, 11 13). *ICANN DNS Engineering*. Retrieved from https://www.icann.org/: https://www.dns.icann.org/

IETF. (2017, 12 16). *The Internet Engineering Task Force (IETF), About the IETF*. Retrieved from IETF: http://www.ietf.org/about/

Inspectie Veiligheid en Justitie/ Agentschap Telecom. (2017). *Onderzoek naar de stroomstoring Amsterdam en omstreken 17 Januari 2017.* The Hague: Inspectie Veiligheid en Justitie/ Agentschap Telecom.

Inspectie VenJ/ Agentschap Telecom. (2015). *Stroomstoring Noord-Holland 27 Maart 2015, Lessen uit de crisisbeheersing en telecommunicatie.* Den Haag: Inspectie Veiligheid en Justitie/ Agentschap Telecom.

ISO. (2017, 12 18). *International organization for standardization, About ISO*. Retrieved from ISO.org: https://www.iso.org/about-us.html

ISO/IEC. (2016). *Information technology - Security techiques - Information security management systems - Overview and vocabulary.* Geneva: ISO/IEC.

ITU. (2017, 12 15). *International Telecommunication Union, Committed to connecting the world*. Retrieved from International Telecommunication Union: https://www.itu.int/en/Pages/default.aspx

Jorritsma-Lebbink, A., & Zalm, G. (1998). *Wijziging van de Machtigingswet Koninklijke PTT Nederland N.V. en enige andere wetten in verband met de juridische splitsing van Koninklijke PTT Nederland N.V.* The Hague: Dutch Government.

Kadaster. (2017, 10 31). *klic-Wion*. Retrieved from Kadaster: http://www.kadaster.nl/klic-wion

Kamp, H. (2014). *Voortgangsrapportage uitwerking visie op telecommunicatie, media en internet*. Directoraat Generaal Energie, Telecom en Mededinging. The Hague: Ministerie van Economische Zaken. Retrieved from https://www.agentschaptelecom.nl: https://www.agentschaptelecom.nl/algemeen/over-agentschap-telecom/programma-telekwetsbaarheid

Kamp, H. (2017). *Brief van de minister van economische zaken 30821 Nationale veiligheid*. The Hague: Ministerie cvan Economische Zaken.

Kamp, H. (2017). *Overnames van Bedrijven*. The Hague: Ministerie van Economische Zaken.

Kaufman, G. G. (2013). *Too big to fail in banking: What does it mean?* LSE Financial Markets Group.

Kist, R. (2017, 01 17). *Noren stoppen met FM, maar Nederland is nog niet zover*. Retrieved from NRC: https://www.nrc.nl/nieuws/2017/01/17/noren-stoppen-met-fm-maar-nederland-is-nog-niet-zover-6231012-a1541547

Klimburg, A., Hathaway, M., Luiijf, E., Healey, J., Lindstrom, G., Ekstedt, V.,... Clemente, D. (2012). *National Cyber Security Framework Manual*. Tallinn, Estonia: NATO CCD COE Publications.

Knol, P., & Zwenne, G. (2015). *Tekst & Commentaar; Telecommunicatie- en privacyrecht*. Deventer: Wolters Kluwer.

KPN. (2017, 10 25). *Sneller Internet Buitengebied De oplossing voor traag internet*. Retrieved from http://www.kpn.com: https://www.kpn.com/thuis/internet-buitengebied.htm

KPN. (2017, 10 13). *Vaste Netwerk*. Retrieved from KPN.com: https://overons.kpn/nl/kpn-voor-nederland/ons-netwerk/vaste-netwerk

Kronieger, R. (2013, 01). Noodcommunicatievoorziening. *Intercom, 2013*(1), p. 4.

Kroon, P., Plückebaum, T., Sanchez Garcia, J., Sabeva, D., & Zoz, K. (2017). *Study into the current and future technological access options to all fixed telecommunication infrastructures in the Netherlands*. Bad Honnef: WIK-Consult GmbH.

Logius. (2016). *Certification Practice Statement (CPS) Policy Authority PKIoverheid voor certificaten uit te geven door de Policy Authority van de PKI voor de overheid*. The Hague: Logius, Ministerie van Binnenlandse Zaken en koninkrijkrelaties.

Luchtvaartnieuws.nl. (2017, 11 13). *Apache vliegt tegen hoogspanningskabel*. Retrieved from Luchtvaartnieuws.nl: https://www.luchtvaartnieuws.nl/nieuws/categorie/4/militair/apache-vliegt-tegen-hoogspanningskabel

Luiijf, E., & Klaver, M. (2015). Governing critical ICT: ELements that require attention. *Symposium on Critical Infrastrucure*, (p. 8). Washington.

Luiijf, E., Burger, H., & Klaver, M. (2003). *Critical Infrastructure Protection in the Netherlands: A quick scan*. The Hague: TNO Physics and Electronics Laboratory.

Luiijf, E., Klaver, M., Nieuwenhuijs, A., Eeten, van, M., & Cruz, E. (2008). *Emperical findings on critical infrastructures dependencies in Europe*. TNO.

Luiijf, H., & Klaver, M. (2000). *In bits and pieces: Vulnerabilities of the Dutch ICT-infrastructure and the consequences for the Information Society*. Amsterdam: Infodrome.

Luiijf, H., Nieuwenhuijs, A., & Klaver, M. (2008). *Critical Infrastructure Dependencies 1-o-1*. The Hague: TNO.

Maersk. (2017, 07 12). *Maersk Advisory Update*. Retrieved from A.P. Moller - Maersk: http://www.maersk.com/en/operationalupdate/general-information

Maij-Weggen, J. (1993). *Wijziging van de Machtigingswet PTT Nederland NV in verband met de opheffing van de verplichting tot opsplitsing van PTT Telecom BV*. The Hague: Minister van Verkeer en Waterstaat.

Meijs, van der, S. (2011, 09 27). *Lektober: iedere dag een privacylek op Webwereld*. Retrieved from Webwereld: http://webwereld.nl/security/54847-lektober-iedere-dag-een-privacylek-op-webwereld

Merriam-Webster. (2017, 12 29). *Definition of Effective*. Retrieved from Merriam-Webster: https://www.merriam-webster.com/dictionary/effective

Merriam-Webster. (2017, 12 29). *Definition of Sufficient*. Retrieved from Merriam-Webster: https://www.merriam-webster.com/dictionary/sufficient

Meulen, van der, R. (2017, 02 07). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*. Retrieved from Gartner: https://www.gartner.com/newsroom/id/3598917

Microsoft Azure. (2017, 12 18). *Azure Datacenters*. Retrieved from http://azure.microsoft.com: https://azure.microsoft.com/nl-nl/overview/datacenters/

Ministerie van Defensie. (2017). *ABDO 2017*. The Hague: Ministerie van Defensie.

Ministerie van Defensie. (2017, 12 18). *Cyber Security*. Retrieved from Ministerie van Defensie: https://www.defensie.nl/onderwerpen/cyber-security

Ministerie van Economische Zaken. (2017, 02 16). *Kabinet wil wettelijke voorwaarden voor overnames telecomsector*. Opgeroepen op 04 12, 2017, van http://www.rijksoverheid.nl: https://www.rijksoverheid.nl/actueel/nieuws/2017/02/16/kabinet-wil-wettelijke-voorwaarden-voor-overnames-telecomsector

Ministerie van Economische Zaken en Klimaat. (2017). *Nota Mobiele communicatie 2017*. The Hague: Dutch Government.

Minkels. (2015). *Vodafone Nederland kiest voor datacenter infrastructuur van Interconnect en Minkels*. Retrieved from http://www.minkels.com: https://www.minkels.com/images/hGxf1

Nationaal Cyber Security Center. (2017, 09 23). *Nationale Cyber Security Strategie*. Retrieved from Nationaal Cyber Security Center: https://www.ncsc.nl/organisatie/nationale+cybersecurity+strategie

National Coordinator for Security and Counterterrorism. (December 2016). *Resilient Critical Infrastructure*. Ministry of Security and Justice. The Hague: National Coordinator for Security and Counterterrorism (NCTV).

NCSC. (2016). *Cybersecuritybeeld Nederland CSBN 2016*. The Hague: Nationaal Cyber Security Centrum.

NCSC. (2017). *Beschrijving producten en diensten NCSC, versie 1.1*. The Hague: Nationaal Cyber Security Centrum.

NCSC. (2017, 12 18). *ICT Response Board*. Retrieved from NCSC.nl: https://www.ncsc.nl/samenwerking/ict-response-board.html

NCSC. (2017, 09 23). *Wat is het NCSC*. Retrieved from Nationaal Cyber Security Centrum: https://www.ncsc.nl/organisatie

NCTV. (2014). *Nationale Cybersecurity Strategie 2, Van bewust naar bekwaam*. The Hague: Ministerie van Veiligheid en Jusitie.

NCTV. (2015). *Nationale Veiligheid en crisisbeheersing (Thema: Herijking vitale infrastructuur)*. The Hague: Nationaal Coördinator Terrorisme en Veiligheid.

NCTV. (2016). *Nationaal Handboek Crisis Besluitvorming*. The Hague: NCTV.

NCTV. (2017, 09 17). *Vitale infrastructuur*. Retrieved from Nationaal Coördinator Terrorisme en Veiligheid: https://www.nctv.nl/organisatie/nationale_veiligheid/vitale_infrastructuur/index.aspx

NCTV. (2017, 12 19). *Vitale Infrastructuur*. Retrieved from Nationaal COördinator Terrorisme en Veiligheid: https://www.nctv.nl/organisatie/nationale_veiligheid/vitale_infrastructuur/index.aspx

Nederland ICT. (2014, 12 11). *Nederland heeft wereldprimeur met noodvoorziening voor langdurige storing mobiel telefoonverkeer*. Retrieved from Nederland ICT: https://www.nederlandict.nl/news/nederland-heeft-wereldprimeur-met-noodvoorziening-voor-langdurige-storing-mobiel-telefoonverkeer/

NetbeheerNederland. (2017, 11 09). *Betrouwbaarheid*. Retrieved from Netbeheernederland.nl: https://www.netbeheernederland.nl/dossiers/betrouwbare-energievoorziening-23

NMA, Opta, V&W. (2001). *Gezamenlijke aanleg en gebruik van UMTS netwerkonderdelen*. The Hague: NMA, Opta, V&W.

NOS. (2012, 02 09). *Hoogste alarmfase na hack KPN*. Retrieved from NOS: http://nos.nl/artikel/339192-hoogste-alarmfase-na-hack-kpn.html

Ofcom. (2011). *Guidelines on the use of battery back-up to protect lifeline services delivered using fibre optic technology*. London: Ofcom.

Onderzoeksraad voor Veiligheid. (2009). *Draadaanvaring Apache helicopter, Bommelerwaard, 12 December 2007.* The Hague: Onderzoeksraad voor Veiligheid.

Oxford University Press. (2017, 12 29). *Definition of Regulation.* Retrieved from Oxford Dictionaries: https://en.oxforddictionaries.com/definition/regulation

P3. (2016). *The 2016 Mobile Network Test in the United Kingdom.* P3.

P3. (2017). *The 2017 P3 Connect Mobile Benchmark in The Netherlands.* P3.

Prins, C. (2011, 09 05). *Een hack bij DigiNotar*. Retrieved from Nederlands Juristenblad: http://njb.nl/blog/import/een-hack-bij-diginotar.9002.lynkx

Prins, J. (2011). *DigiNotar Certificate Authority breach "operation Black Tulip".* Delft: Fox-IT.

Rechtbank Den Haag. (2017). *ECLI:NL:RBDHA:2017:10789 Vordering Brein tot voorlopige blokkade van de website The PirateBay voor abonnee's van Ziggo en XS4ALL toegewezen, gelet op oordelen rechtbank, Hoge Raad en Hof van Justitie EU in bodemprocedure.* The Hague: Rechtbank Den Haag.

Reijerman, D. (2011, 05 12). *KPN past deep packet inspection toe op mobiel internetverkeer*. Retrieved from http://www.tweakers.net: https://tweakers.net/nieuws/74419/kpn-past-deep-packet-inspection-toe-op-mobiel-internetverkeer.html

Rekenkamer Rotterdam. (2017). *In onveilige handen.* Rotterdam: Rekenkamer Rotterdam.

Resnick, P. (2014). *RFC-7282 On consensus and Humming in the IETF.* IETF.

Rijksoverheid.nl. (2013, 01 13). *Reactie n.a.v. Brandpunt uitzending over 112*. Retrieved from https://www.rijksoverheid.nl: https://www.rijksoverheid.nl/actueel/nieuws/2013/01/13/reactie-n-a-v-brandpunt-uitzending-over-112

Rijksoverheid.nl. (2017, 07 11). *Eerste Kamer stemt in met nieuwe Wet op de inlichtingen- en veiligheidsdiensten*. Retrieved from Rijksoverheid.nl: https://www.rijksoverheid.nl/onderwerpen/bevoegdheden-inlichtingendiensten-en-veiligheidsdiensten/nieuws/2017/07/11/eerste-kamer-stemt-in-met-nieuwe-wet-op-de-inlichtingen--en-veiligheidsdiensten

Rijksoverheid.nl. (2017, 12 18). *Ministeries*. Retrieved from Rijksoverheid.nl: https://www.rijksoverheid.nl/ministeries

Rittel, H., & Webber, M. (1973). *Dilemmas in a General Theory of Planning.* Amsterdam: Elsevier Scientific Publishing COmpany.

Rogers, M., & Ruppersberger, D. (2012). *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE.* Washington: U.S. House of Representatives.

Rousseau, J.-J. (1762). *Du contrat social ou Principes ud droit politique.*

RTL Nieuws. (2017, 04 04). AIVD: Rusland probeerde met nepnieuws onze verkiezingen te beïnvloeden. *RTL Nieuws*, p. 1. Retrieved 04 15, 2017, from https://www.rtlnieuws.nl/nederland/politiek/aivd-rusland-probeerde-met-nepnieuws-onze-verkiezingen-te-beinvloeden

Runhaar, H., Kasper Gilissen, H., Uittenbroek, C., Mees, H., Rijswick, van, M., & Gerretsen, A. (2014). *Publieke en private verantwoordelijkheden voor klimaatadaptatie.* Utrecht: Universiteit Utrecht.

Ryan, P. S., & Gerson, J. (2012). *A primer on Internet Exchange Points for Policymakers and non-engineers.* Catholic University of Leuven, University of Colorado at Boulder: Social Science Research Network.

Schellevis, J. (2012, 01 03). *2011: van netneutraliteit tot downloadverbod*. Retrieved from http://www.tweakers.net: https://tweakers.net/reviews/2432/2/2011-van-netneutraliteit-tot-downloadverbod-dpi-en-voip.html

Schellevis, J. (2017, 05 04). Nederland krijgt minder nieuwe glasvezelverbindingen. *NOS*, 1. Retrieved 05 04, 2017, from http://nos.nl/artikel/2171385-nederland-krijgt-minder-nieuwe-glasvezelverbindingen.html

Schmitt, M. N. (2013). *Tallinn Manual on the international law applicable to cyber lawfare.* Tallinn: Cambridge University Press.

Schneier, B., & Ellison, C. (2000). Ten Risks of PKI: What You're not Being Told about Public Key. *Computer Security Journal*, 7.

Seba, T., & Arbib, J. (2017). *Rethinking Transportation 2020-2030, The Disruption of Transportation and the Collapse of the Internal-Combustion Vehicle and Oil Industries.* RethinkX.

Security.nl. (2012, 10 04). *Hoe providers weten dat je computer besmet is*. Retrieved from http://www.security.nl: https://www.security.nl/posting/38285/Hoe+providers+weten+dat+je+computer+besmet+is

SIDN. (2017, 12 18). *Over SIDN*. Retrieved from Stichting Internet Domeinregistratie Nederland: https://www.sidn.nl/t/over-sidn

Sires, A., & Duncan, J. (2017, 04 06). Letter to secretary of treasury regarding Citgo. Washington, District of Columbia, United States of America. Retrieved from http://jeffduncan.house.gov/sites/jeffduncan.house.gov/files/documents/Duncan-Sires%20PDVSA-Rosneft-Citgo%20Letter%20%284.6.17%29.pdf

Smith, B. (2017, 05 14). *The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack*. Retrieved from http://blogs.microsoft.com: https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

Spamhaus.org. (2017, 12 06). *The Domain Blocklist*. Retrieved from Spamhaus.porg: https://www.spamhaus.org/dbl/

Sprado, A. (2017, 09 29). *Randstad gaat volledig naar cloud met AWS*. Retrieved from https://www.computable.nl: https://www.computable.nl/artikel/nieuws/cloud-computing/6213370/250449/randstad-gaat-volledig-naar-cloud-met-aws.html

Statista. (2017, 11 23). *Most famous social network sites worldwide as of September 2017, ranked by number of active users (in millions)*. Retrieved from Statista: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Statista. (2017, 12 29). *Ranking of countries with best infrastructure in 2017.* Retrieved from Statista, the statistics Portal: https://www.statista.com/statistics/264753/ranking-of-countries-according-to-the-general-quality-of-infrastructure/

Steur, van der, G. (2016). *Voortgangsbrief Nationale Veiligheid.* The Hague: Ministerie van Veiligheid en Justitie.

Stichting COIN. (2017, 12 18). *Nummerportabiliteit*. Retrieved from COIN: https://coin.nl/nl/diensten/nummerportabiliteit

Storingsoverzicht.nl. (2014, 11 08). *Storing Elektronische Programma Gids van Interactieve TV*. Retrieved from Storingsoverzicht.nl: https://storingsoverzicht.nl/2014/kpn-storing/storing-elektronische-programma-gids-interactieve-tv/

Stratix. (2017). *Breedband in de OOV sector in de 700 MHz Band, onderzoek naar behoefte aan mobiele breedband datacommunicatie.* Hilversum: Stratix.

Telecompaper. (2017, 11 16). *T-Mobile zet 60 minuten noodstroom bij mobiele sites*. Retrieved from Telecompaper: https://www.telecompaper.com/nieuws/t-mobile-zet-60-minuten-noodstroom-bij-mobiele-sites--1220665

Toonk, A. (2017, 12 12). *Popular destinations rerouted to Russia*. Retrieved from BGPMON: https://bgpmon.net/popular-destinations-rerouted-to-russia/

Veen, J. (2017). *Essence of Encryption, A case study of the nascence of the Dutch government position on encryption.* The Hague: Cyber Security Academy.

Veiligheidsregio Gelderland Zuid. (2017, November 23). *Crisiscommunicatie*. Retrieved from Veiligheidsregio Gelderland Zuid: http://www.vrgz.nl/voor-inwoners/crisiscommunicatie/

Veiligheidsregio Gelderland Zuid. (2017, 11 14). *Stroomstoring vervolg*. Retrieved from Veiligheidsregio Gelderland Zuid: http://www.vrgz.nl/nieuws/stroomstoring-vervolg/
Veiligheidsregio Gelderland Zuid. (2017, 11 13). *Stroomstoring Zoelmond en omgeving*. Retrieved from Veiligheidsregio Gelderland Zuid: http://www.vrgz.nl/nieuws/stroomstoring-zoelmond-en-omgeving/
Verizon. (2017). *2017 Data Breach Investigations Report, 10th edition.* Verizon.
VERON. (2017). *Noodcommunicatie*. Retrieved from http://www.veron.nl: https://www.veron.nl/activiteiten/noodcommunicatie/
VEWIN. (2017, 11 09). Retrieved from VEWIN.nl: http://www.vewin.nl/vewin-den-haag/activiteiten/
VGRZ. (2017, 11 20). *Uitval Stroom*. Retrieved from http://www.vgrz.nl: http://www.vrgz.nl/wat-te-doen/uitval-stroom/
VRGZ. (2017, 11 20). *OOV Alert*. Retrieved from http://www.vrgz.nl: http://www.vrgz.nl/voor-partners/oov-alert/
Vroegop, B. (2017, 12 15). *'Onzeker of overname Tele2 door T-Mobile mag doorgaan'*. Retrieved from Nu.nl: https://www.nu.nl/mobiel/5050994/onzeker-of-overname-tele2-t-mobile-mag-doorgaan.html
VVD, CDA, D66 en ChristenUnie. (2017). *Vertrouwen in de toekomst, Regeerakkoord 2017-2021.* The Hague: VVD, CDA, D66 en ChristenUnie.
WABP. (2017, 09 03). *welkom bij WABP Nederland en België*. Retrieved from WhatsApp Buurt Preventie: https://wabp.nl/
Wikipedia. (2017, 12 18). *List of technical standard organisations*. Retrieved from WIkipedia: https://en.wikipedia.org/wiki/List_of_technical_standard_organisations
Wikipedia. (2017, 10 13). *Wijkcentrale*. Retrieved from Wikipedia: https://nl.wikipedia.org/wiki/Wijkcentrale
Wolff, J. (2016, 12 21). *How a 2011 Hack You've Never Heard of Changed the Internet's Infrastructure*. Retrieved from Future Tense: http://www.slate.com/articles/technology/future_tense/2016/12/how_the_2011_hack_of_diginotar_changed_the_internet_s_infrastructure.html
World Economic Forum. (2016, 11 24). *This map shows how undersea cables move internet traffic around the world*. Retrieved from World Economic Forum: https://www.weforum.org/agenda/2016/11/this-map-shows-how-undersea-cables-move-internet-traffic-around-the-world/
www.overheid.nl. (2017, 02 16). *Wet ongewenste zeggenschap telecommunicatie.* Retrieved from http://www.overheid.nl: https://www.internetconsultatie.nl/telecommunicatie/details
www.samentegencybercrime.nl. (2008). *Gedragscode Notice-and-take-down.* The Hague: Ministerie van Economische Zaken en Klimaat.

10 Terms and Abbreviations

AMvB	Algemene Maatregel van Bestuur (General governmental regulation)
AT	Governmental Audit department Telecommunication Infrastructure (Agentschap Telecom)
BZK	Ministry of the Interior and Kingdom Relations (Binnenlandse Zaken en Koninkrijksrelaties)
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CPS	Certificate Practice Statement
DARES	Dutch Amateur Radio Emergency Services

DCC	Departmental Crisis Centre (Every government ministry has a crisis centre)
DNS	Domain Name System
DNSSEC	Domain Name System with built in security functionality
eIDAS	Regulation on electronic identification and trust services for electronic transactions in the internal market.
EECC	European Electronic Communications Code
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications and Standardisation Institute
EZK	Ministry of Economic Affairs and Climate Policy (Economische Zaken en Klimaat)
GDPR	Generic Data Protection Regulation
ICCB	Interdepartmental Commission Crisis Management (Interdepartementale Commissie Crisis Beheersing)
IETF	Internet Engineering Task Force
IoT	Internet of Things
IRB	ICT Response Board (Public Private)
ISAC	Information Sharing and Analysis Centre
ISP	Internet Service Provider
ITU	International Telecommunication Union
J&V	Ministry of Justice and Security (Justitie en Veiligheid)
MCCB	Ministerial Commission Crisis Management (Ministeriële Commissie Crisis Beheersing)
NATO	North Atlantic Treaty Organization
NCC	National Crisis Centre
NCSC	National Cyber Security Centre (Nationaal Cyber Security Centrum)
NCO(-T)	National Continuity Council (Nationaal Continuïteitsoverleg(-Telecommunicatie))
NCTV	National Coordinator for Security and Counterterrorism
NCV	Nationale Continuïteitsvoorziening
NIS	Directive on Network and Information Systems
OT2000	Governmental telephony services
OTT	Over-the-Top (providers delivering services on top of traditional telecommunications infrastructure)
TLD	Top Level Domain
VERON	Vereniging voor Experimenteel Radio Onderzoek Nederland (Dutch organisation for radio research)

11 Interview details

11.1 Introduction letter to interviewees

This part contains the letter (in Dutch) to the parties invited to be interviewed. Some of the letters were slightly adapted in case of authors knowing the interviewee.

Beste lezer,

Bij deze wil ik vragen of u mee wilt werken aan een interview met betrekking tot overheidsregulering in relatie tot de robuustheid van telecommunicatievoorzieningen.
Belangrijke telecommunicatiediensten zoals internettoegang, vast en mobiel bellen en televisiediensten zijn vitale onderdelen van de Nederlandse infrastructuur en de Nederlandse overheid stelt eisen en normen om deze infrastructuren veilig, betrouwbaar en beschikbaar te houden. Aangezien deze infrastructuren eigendom zijn van private partijen en ook door deze partijen (of door onderaannemers) worden geëxploiteerd is er sprake van een complexe balans.

Voor mijn thesis aan de Cyber Security Academy (https://www.csacademy.nl/) ben ik aan het onderzoeken of de overheidsmaatregelen om deze telecommunicatiediensten robuust te houden voldoende zijn of dat er meer moet gebeuren. Een belangrijk onderdeel van mijn onderzoek is om vast te stellen hoe diverse belanghebbende partijen hier tegen aan kijken zodat een beeld gegeven kan worden van de situatie met betrekking tot wet- en regelgeving omtrent telecommunicatiediensten. Onder de partijen die ik wil interviewen bevinden zich overheidsinstellingen, telecommunicatie-dienstverleners en gebruikersverenigingen.

Dit interview van ongeveer een uur lang wil ik indien mogelijk persoonlijk afnemen en tijdens het interview maak ik wel notities, maar er zullen zeker geen opnames worden gemaakt. Citeren van uitspraken gebeurt in overleg en u krijgt de publicatie ook te lezen voordat deze gepubliceerd gaat worden zodat eventuele omissies gecorrigeerd kunnen worden.
Deze studie doe ik naast mijn werk als security architect bij KPN. In mijn thesis besteed ik dan ook veel aandacht aan het voorkomen van vooringenomenheid met betrekking tot het gehele speelveld van telecommunicatiewetgeving en diensten in Nederland en hoop veel van de interviews te leren.

Tijdens het interview hoop ik dat de volgende hoofdzaken aan bod kunnen komen:
- Vind u dat de overheid en de telecommunicatiedienstenleveranciers voldoende doen om de telecommunicatie infrastructuren te beschermen.
- Wat moet er naar uw beeld verbeteren en aangepast worden vanuit het overheidsperspectief?

Ik ben benieuwd naar uw antwoord.

Met vriendelijke groeten,
Erik van Garderen

11.2 Parties interviewed

The following people have been interviewed (mentioned in Alphabetical order)

- Gerard van Eldik (Owner, Aemotion, CulemborgZo), Culemborg Aemotion Office, 2017-11-17
- Frank Jansen (Business Continuity Manager, KPN), The Hague, KPN Office, 2017-11-13
- Paul Knol (Scholar, Universiteit Leiden and Legal & Regulatory, KPN)
- Walter Kroezen (Regulatory Advisor, Vodafone), Maastricht, Vodafone Office, 2017-12-08

- Ronald van der Luit (Chairman NCO-T, EZK), The Hague, EZK Office ,2017-11-02
- Willem Schuringa (Network Architect, ASR), Utrecht, ASR Office, 2017-12-08
- Ivor Trynes(Risk Manager, Vodafone), Maastricht, Vodafone Office, 2017-12-08
- Dirk Ytsma (Consultant, Agentschap Telecom), Amersfoort, AT Office, 2017-10-27

12 Ranking of infrastructure

The table below gives the ranking of infrastructure quality as reported by Statista for the first 40 countries out of the report ranking over 100 countries [Sta171]. Ranks, names and scores are given in the exact order as in the Statista graph: "*The scale ranges from 1 = underdeveloped and 7 = extensively by international standards*."[Sta171]. Note that this ranking is based not only on electricity and telecommunications infrastructure, but also on civil engineering infrastructure, such as roads, ports etc.

Rank	Country	Value
1	Switzerland	6,6
2	Hong Kong SAR	6,4
3	Singapore	6,4
4	Japan	6,2
5	Netherlands	6,2
6	United Arab Emirates	6,2
7	Finland	6,1
8	France	6,1
9	Austria	5,9
10	United States	5,9
11	Denmark	5,8
12	Germany	5,7
13	Korea Rep.	5,7
14	Portugal	5,7
15	Iceland	5,6
16	Luxembourg	5,6
17	Sweden	5,6
18	Spain	5,5
19	Estonia	5,4
20	Taiwan, China	5,4
21	Malaysia	5,3
22	Bahrain	5,2
23	Canada	5,2
24	Norway	5,2
25	Qatar	5,2
26	Azerbaijan	5
27	Turkey	5
28	United Kingdom	5
29	Belgium	4,9
30	Israel	4,9
31	Lithuania	4,9
32	Oman	4,9
33	Saudi Arabia	4,9
34	New Zealand	4,8
35	Australia	4,7
36	Chile	4,7
37	Croatia	4,7
38	Cyprus	4,7
39	Morocco	4,7
40	Panama	4,7