Essence of Encryption

A case study of the nascence of the Dutch Government position on encryption

CYBER SECURITY ACADEMY

Jeroen Veen

S1728016

January 2017

Preface

This is a case study into the Dutch Government's position on encryption, presented by the author as a master thesis at the Cyber Security Academy, a curriculum developed in collaboration with Leiden University, Delft University of Technology and The Hague University of Applied Sciences.

Abstract

Following several terrorist strikes in the EU and several high-profile police cases in the US, an international debate about encryption has sprung up, again. This debate focuses on which types of encryption should be available to the general public and whether or not government agencies should have access to the public's encrypted data, by means of a special access backdoor. From the point of view of investigative agencies encryption renders communications between criminal and terrorist actors unreadable, leading them to state they are 'Going Dark' because of encryption. Digital rights movements and academics point out the inherent effects to not only criminals and terrorists but everyone on the Internet when governments start interfering with encryption.

Encryption, as a technology to send messages that cannot be understood when intercepted, is old, ancient even. Likewise, the desire to still be able to understand these messages are equally ancient. Special access for government agencies has been debated and regulated in times of postal, phone and now Internet communications. In fact, a scenario that is very reminiscent of todays was played out in the 1990's, when the Clinton administration proposed to fit a chip into mobile phones that allowed government agencies to bypass encryption of mobile voice calls. The, mostly US centric, debate that ensued is now referred to as the (first) 'Crypto Wars'.

In our research into this subject we answer our research question '*How can we understand the decision-making of political actors in the Dutch public sector within the encryption debate?*' by recognising that there are multiple viewpoints one can take. Advantages and disadvantages of backdoors look different when viewed through economic, national security or privacy lenses. Applying these lenses to what is known of government's positions in this debate is presented in a quick scan of government positions, which predominantly shows that there are very few countries that have come to an official position in light of this re-emerging debate. Those that do have rules and regulations often fall into, from a West-European point of view, more authoritarian regimes. There is one notable exception.

The Netherlands surprised much of the world (and perhaps itself) when the Cabinet position on encryption, backing strong encryption and opposing the addition of backdoors, was published early in 2016. Questions from members of the Dutch Parliament to the Minister for Security and Justice and the Minister for Economic Affairs led to Cabinet wide deliberations, culminating in a statement that there should be no government interference in encryption technologies. Though the position is understanding towards problems investigative agencies have due to modern ways of communication, the end conclusion is that this cannot be aided without detrimental effect to society at large.

In the answering of our second research question '*What process and factors within the Netherlands contributed to the forming of the Dutch official position on encryption?*' we conclude that the Netherlands has been able to come to an official position due to a combination of factors: critical members of parliament (in a niche-enabling many party system) that challenge government statements about encryption and possible weakening of it; A willingness to understand viewpoints from differing points of view, including those of digital rights movements (a balance in the lenses through which to view the problem); The desire to come to an agreement (perhaps an influence of

the Dutch “Poldermodel”). A large telecommunications sector that is dependent on the Netherlands’ central position for Internet traffic was also found to be a factor, though this is not unique for the Netherlands.

Though these factors can be abstracted and taken into consideration by other countries that see a need to come to an official position, copying of what was done in the Netherlands is no mean feat. Ultimately this becomes more a question of public administration and social and cultural history than a question of cyber security, however well we define lenses through which to analyse the debate. This means a third research question we had defined ‘*To what extent can success factors for the development of an official position be derived from the Dutch case?*’ remains largely unanswered and thus open for future work, not in the least place due to our research having analysed only the Dutch case.

Combining our findings, we ultimately conclude understanding of the encryption debate is increased when differing viewpoints (economic, national security and privacy) are understood in their own right and that this, together with the factors mentioned earlier, is also what allowed the Netherlands to come to a government position on encryption.

The debate surrounding encryption is active and lively and will not go away anytime soon. Though the current ‘Crypto Wars’ may end once the world gets either more control over, or gains more acceptance of, current terrorist situations we can expect that these Wars will get another instalment. The same type of discussion can be expected to resurface when next we move to a different form of communicating that yet again threatens intelligence agencies with ‘Going Dark’.

Table of Contents

I. Introduction 6
II. Research question 7
III. Research methodology 8
I. Desk Research / Literature study 8
II. Interviews 9
III. Limitations and final remarks 11
IV. A primer on encryption in communications 13
I. A short history of encryption backdoors 13
II. Current debate 17
V. Viewpoints on encryption 26
I. The economic lens 28
II. The national security lens 30
III. The privacy lens 32
IV. Reflections on this model 35
VI. The Netherlands and its official position 36
I. Process and formation of Cabinet position 37
II. Results of the process 44
VII. Findings 45
VIII. Conclusions & future work 46
Appendix 1: interview questions 49
Appendix 2: interview details 50
Bibliography 51

I. Introduction

One of the fundamentals underlying cyber security is encryption. Encryption methodologies allow us to store and transmit data in such a way that only those in possession of a specific bit of information (the encryption key) are able to access that information. Applications that are built on top of this allow us to communicate securely (e.g. by means of encrypted emails or Whatsapp[1] messages) or otherwise share information securely for day to day financial reasons (e.g. online shopping and banking).

Following terrorist attacks in 2015 and 2016 politicians in several nations[2] have started a public debate, proposing to add backdoors to our encryption, allowing government (police or security services) access to encrypted content by use of a specific key (a golden key).

Throughout this thesis, and the literature much of its research is based on, there are a couple of different technical concepts that essentially entail the same thing from a government access point of view. Encryption backdoors, key-escrow, 'golden keys' and special access, while having different modus operandi all represent methods through which a third party (usually a government) can gain access to information being shared between two parties. This type of access is different from existing wire-tapping and eavesdropping capabilities that exist for police forces and secret services. A wiretap will simply copy all information to a third party, when the persons whose communications are copied apply encryption to their communications the wiretap still works, but the data obtained in this manner is now useless. To again make use of the information in the communications' data the encryption would somehow have to be removed. It is the latter removal of encryption that is the subject of the debate our thesis focuses on.

This debate is being conducted with a clear division between proponents and opponents. On the one side we have proponents arguing that, in this day and age, the fact that many communications are encrypted by default form a hindrance for government investigations into criminal and terrorist activities. They argue that encryption essentially hinders said agencies to help protect society. On the other side opponents of backdoors in encryption note the impossibility of adding a backdoor that is uniquely usable by government agencies (because criminals and terrorists can use them as well), along with principal objections to the notion that this is at all necessary 'in this day and age'.[3]

This is not the first time this debate has raged (and we will conclude that is most probably not the last). History has seen the discussion between the need for privacy and the need for insights in communications many times but this came to a pinnacle in the nineties of the last century, when cryptographic abilities of cell-phones led to a broad debate in the United States of America. The history of the debate and earlier 'Crypto Wars' are further described in chapter IV.

The current debate is still very much ongoing at the moment of writing (of this thesis). This iteration has seen some interesting things happening in the political arena: several governments have issued statements about the desirability (or not) of backdoors in encryption but, most notably, the Netherlands has issued an official government position which, though it has it's nuances, mostly makes a point against the weakening of encryption (V. der Steur and Kamp 2016).

[1] Which saw the introduction of end-to-end encryption between users in 2016 (Budington 2016)

[2] For example in the US (Feinstein and Burr 2016), in the UK (Bienkov 2015) and in France and Germany (Lomas 2016a).

[3] A good example of this debate unfolding can be found in the 'Going dark' debate as conducted by the US Senate Committee on the Judiciary. (Judiciary 2015)

In this thesis, we propose a model of three lenses through which to look at different positions within this debate: an economic lens, a national security lens and a privacy lens. Equipped with these lenses we have investigated positions of different nations and different actors in this debate. Following this initial categorisation of actors and nations we have gone one step further in the analysis of the Dutch position. Several actors that were expected to have (direct or indirect) roles in the conception of the Dutch official position were interviewed. The results of this were combined to gain understanding on both the process within the Netherlands that lead to an official statement and on factors that aided the creation of said statement.

In our conclusion, we have identified what these factors are in the Netherlands, evaluated what can be learned when applying these lenses and what they have taught us about the factors that lead to the development of the Dutch position, including which of these factors are generalisable in a way that actors in other countries can apply.

II. Research question

While the Netherlands has long had a reputation as a country where individual freedoms are respected it is unclear why a specific declaration about encryption, and the wish to keep encryption methods free from detrimental government interference, has surfaced in the Netherlands and not in other countries.

We can think up various reasons and these form the basis for our research. Was the Dutch Government informed better, leading to more political awareness of the value of encryption? Were there specific proponents of backdoors in encryption present in other countries but absent in the Netherlands? Were specific opponents given a stronger voice (and if so through which means)? Or have there been specific cases or experiments with backdoors in encryption (or comparable other cases) that have lead Dutch policy makers to make a strong statement? Or is this another example of the Dutch political 'Poldermodel'[4]: consensus culture in action?

Before we can analyse any specific nation's position we need a way to understand different positions, turning our first question into one of methodology:

How can we understand the decision-making of political actors in the Dutch public sector within the encryption debate?

This question is answered by the model of lenses through which to look at an actor's behaviour in chapter V (which we will describe from a methodological point of view in the next section). Devising a way to look at different positions within the encryption debate aids us in our case study of the Dutch position on encryption. This case study has the following core questions to answer:

What process and factors within the Netherlands contributed to the forming of the Dutch official position on encryption?

The result of this can be used in answering the following sub-question:

To what extent can success factors for the development of an official position be derived from the Dutch case?

[4] Which has gained enough international fame to earn a well referenced Wikipedia article (https://en.wikipedia.org/wiki/Polder_model)

Defining hypotheses to aid our research was not done as this felt rather forced given the nature of our research. Our aim is to understand the encryption debate, positions in it, and in particular the circumstances surrounding the origination of the Dutch position. We do not have an aim to predict what will come next.

III. Research methodology

From a scientific viewpoint, this thesis will follow a classic approach. Design science that leads to a new method to create policy will not be applied. The "why" part of the research is where the focus lies rather than on a "how can we" level.

The figure below gives a high-level overview of parts of our thesis, with the subsequent paragraphs describing our approach, and its limitations, in more detail.

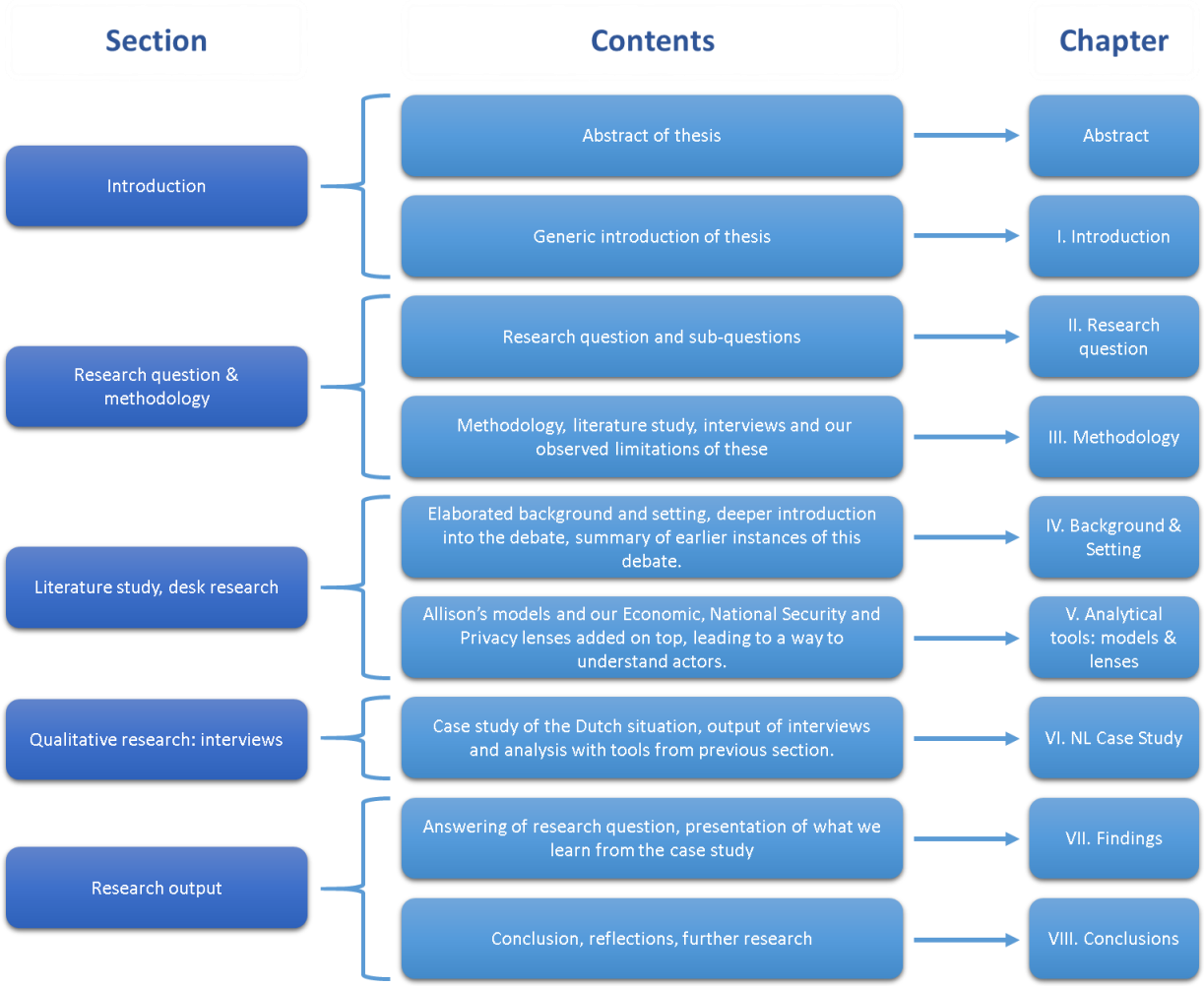

Figure 1: overview of thesis structure

I. Desk Research / Literature study

Several research methods have been applied, depending on the needs of specific parts of our thesis.

The thesis will start with a more detailed look (via literature study) into use of encryption in communications, examining the (mostly recent) past both in the use of encryption and methods to

circumvent it, and the examination of past discussions that were alike. This entailed going through many scholarly and media articles in detail to get to the real research behind it.

To aid a broader understanding we also performed a quick-scan of positions of other countries in this debate. This results in an overview of the current debate, including insights into several government's positions on backdoors in encryption, which also shows why the Netherlands have a special position in this that warrants a case study. To come to this, we followed a desk based qualitative approach where official government publications, statements from government officials and reports of those in the media were used to create an overview of nations and their position on encryption.

To aid our understanding of current affairs we will devise a model to help our first research question: *How can we understand the decision-making of political actors in the Dutch public sector within the encryption debate?* For this we will base ourselves on earlier examples of research that was aimed at understanding positions of different actors within a certain debate. We will mostly use the method devised by Graham Allison, when trying to aid studies into governmental decision-making, in his analysis of the Cuban missile crisis (Allison 1969) as a basis for our own model. There are two reasons for adapting Allison's research to our own case; Firstly, Allison's model allows us to analyse political behaviour through different models (a Rational Actor model, an Organisational Process model and a Governmental Politics model); Secondly, we will add specific lenses to further aid analysis of our case (an economic lens, a national security lens and a privacy lens). This method of working brings us firstly, a certain distance at which to put ourselves whilst analysing the case at hand, and secondly, different angles at which to look at the same situation.

Research into, and supporting, these lenses that add an angle to Allison's models, was done by desk research into several sources, some of whom are scientific (e.g. papers and articles about encryption, effects of backdoors) and some of whom are non-scientific (e.g. government publications, research from those reporting on scientific research and generic news articles and reports).

Armed with historical context, earlier research on encryption (and backdoors) and our lens based model, we have performed a case study of the situation in the Netherlands.

Specific investigation into how the Dutch position on encryption came to be, began with study of sources reporting on the position (e.g. government publications, news sites) but is supported by qualitatively gained information, through the form of interviews with relevant (government) stakeholders.

Notable authors on this subject include Bruce Schneier, Whitfield Diffie and Ross Anderson, who were part of a group of scholars that critiqued US Government endeavours into limitations to encryption, both in earlier and current debates. The creation of our model to do the case study of the Dutch situation is based on, and builds further on, Graham Allison's work. From a media point of view Wired (and especially journalist Andy Greenberg there) and dailydot.com provided the most information about international developments in the encryption debate. Dutch technological news site tweakers.net and Dutch security news site security.nl provided, and keep providing, the most updates on the running debate in the Netherlands and the EU.

II. Interviews

The goal of the interviews was to gain understanding into; How the process to get to an official position works; Who is involved; What deliberations were made; What contributes to the creation of an official positions and what counteracts such creation.

Interviews were conducted in a semi-structured manner, meaning there was a list of subjects but not a fixed form or order these were presented in. Interviewees were presented with subject and research questions of the thesis beforehand but did not receive the list of questions[5]. In the conversations, the research this thesis focuses on was explained and the subjects mentioned in the previous paragraph were discussed.

To allow more open discourse no audio recordings were made of the conversations.[6] Minutes were taken but these are not published in the appendices to this thesis, there was no fixed format for the interviews, leading to discussions that contained remarks that were asked not to be included. The following paragraph gives an overview of parties that were interviewed. For exact details of persons involved contact the author as, for reasons of anonymity, only organisations are mentioned in this overview. For each of the parties interviewed we have described why they are expected to be significant in this process.

Bits of Freedom. Though we have primarily spoken to government representatives Bits of Freedom (BoF) is not a government agency but a digital rights organisation that focuses on digital civil rights. BoF blogs about events in the digital world and presents both solicited and unsolicited advice to those in the digital domain (which includes the government). They also organise the annual Big brother awards[7] in the Netherlands. They are included as an actor to examine what role digital civil rights defenders play in the context of political decision-making. We spoke to Rejo Zenger, who works for BoF in the role of Blogger, advisor and technology expert.

National Cyber Security Centre (NCSC). The NCSC is a part of the Dutch Ministry of Security and Justice and primarily has a role to advise the government on cyber security affairs. We spoke to a technical expert who was present during sessions that led to the Dutch Cabinet position.

Ministry of Security and Justice. The Dutch Cabinet position is an opinion of the government as a whole, but it was signed by ministers of two specific ministries, one of which was the Ministry of Security and Justice. Since this ministry has both national security and public prosecution among its tasks this makes them an important actor. We spoke to a Senior Policy Advisor at the Ministry of Security and Justice.

Ministry of Economic Affairs. The Minister for Economic Affairs was the other signatory of the Cabinet position. Digital infrastructure is a big asset for the Dutch economy, government policy on encryption can have quite an impact on the sector that depends on it. The Ministry of Economic Affairs was included for these reasons. We spoke to Ronald van der Luit, who leads the cluster surrounding continuity, security and privacy for the telecom market, and was present during sessions that led to the Dutch Cabinet position.

Ministry of Defence. The 'cyber' domain has been part of Defence departments the world over, which means that any government position on encryption will have impact on the way in which the cyber division of the department and its intelligence agency can work. The Dutch Military Intelligence

[5] With one exception: due to agenda constraints Bits of Freedom (BoF) requested a phone call instead of a meeting and requested to receive the top questions to BoF beforehand, to make maximum use of what time there was, we agreed.

[6] This is how we had planned this, and rightly so, as some of the talks took place at Dutch ministries where usage of recording equipment is prohibited.

[7] Which includes both negative (the year's biggest privacy offender) and positive (the year's biggest privacy advocate) awards, for more information see (in Dutch): https://bigbrotherawards.nl/over-bba/

and Security Service is also part of this ministry. We spoke to Eelco Karthaus, Senior Policy Advisor at the Ministry of Defence.

Members of Parliament. Several members of the Dutch Parliament, who are responsible for Internet related subjects in their respective parties are initiators of this debate. The parliamentary system mandates the government to answer questions posed to them from parliament, from which follows that parliament members are an actor in this debate. One member of the Dutch Parliament is particularly active on this subject: Kees Verhoeven, who is in the 2nd chamber of the Dutch Parliament for the D66 party. We spoke to Marijn van Vliet, who works for D66 specifically to aid on ICT related subjects and assisted Kees Verhoeven on this subject.

Many more parties have (direct or indirect) influences on the forming of official Cabinet statements, but not all were included in order to come to a more manageable scope. For some actors this warrants some extra explanation.

Other ministries. As our research has shown government positions are agreed upon in the Cabinet, which included several other ministries than the ones interviewed. The ministries not included (Ministry of General Affairs (including the Prime Minister); Ministry of Finance; Ministry of Education, Culture and Science; Ministry of Infrastructure and the Environment; Ministry of Health, Welfare and Sport; Ministry of Social Affairs and Employment) are seen as less directly affected and were therefore not included.

The commercial sector. CISO's and CEO's in the commercial sector also may have had an indirect influence on parties that were at the table during the formation of the Dutch Cabinet position on encryption. We have decided not to include these as we are mainly interested in what ultimately lead to the formation of a Cabinet position and not necessarily in all the influences on the Cabinet per se, which would lead our research farther away from cyber security governance into the domain of public administration.

The summary of the goal of the research and the questions addressed in the interviews can be found in Appendix 1. Appendix 2 contains an overview of parties that were interviewed. Minutes of the interviews are available from the author on request.

Our approach of combining desk based literature study and interviews culminated in a flow for this document as depicted in the figure below.

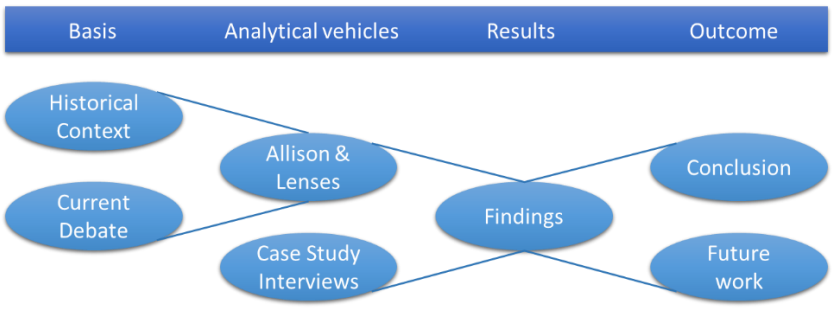

Figure 2: overview of research flow

III. Limitations and final remarks

Any research approach will encounter limitations and ours is no exception. Whilst Allison had information from a wide variety of sources within the respective governments we find ourselves at more distance or, where we are not at a distance in our interviews, we have only spoken to a limited set of people. In relation to Allison's models we find ourselves rather heavily focused on the Rational

Actor model, with some glances into the underlying Organisational Process model and occasional insight into the more personal viewpoints that relate to the Governmental Politics model.

As we build our ways of analysis of the Dutch situation on top of Allison's model we are also burdened with the critique on Allison's work, not in the least his own mention of falsifiability problems of analysis from a rational actor's point of view. Furthermore, In the early nineties a more detailed critique of Allison's work was presented by Bendor and Hammond , who stated "*Most importantly, there is an inevitable tension between attempting to explain a particular event (a task characteristic of historians) and attempting to construct models (a job more characteristic of social scientists)*"(Bendor and Hammond 1992, 318). This is a tension we also encounter in our research so we must recognise that "*The demands of specialization, of allocating one's limited time either to investigating particular historical facts or to developing the mathematical expertise needed in model building, imply that this trade-off is a difficult one*" (Ibid., 318).

Knowing this, we proceed with the notion that we want to understand better how the encryption point of view came to be, not necessarily in why policymakers were motivated the way they were. In other words: we should note that while our research sheds light on the nascence of the Dutch position on encryption it does not necessarily form the best scientific approach towards analysis of policy making in general.

Another limitation emerged during our literature study into the lenses we add to Allison's model in order to understand what factors may bind one's rationality. Economy, national security and privacy viewpoints all have a basis in existing ideas and research: the choice of these three angles reflects ideas from media, research and is reflected in statements from our interviewees. However, academic sources are, in general, much more supportive of ideas from a privacy and economic viewpoint than one of national security. It only takes a first glance to note that most academic research is in critique of concepts that make use of backdoors or key escrow. A proponent of a national security view may find elements of our thesis one-sided but the reality is that this is not our choice or opinion but a valid reflection of available sources.

Like our literature study our interviews present us with some limitations. We spoke to a select group of people, six actors varying from partaker of the Cabinet sessions on the subject (e.g. the representative of the Ministry of Economic Affairs) to individuals not directly partaking and not part of the government (e.g. Bits of Freedom). We do have first-hand information on the formation of the Dutch position but we have not spoken to all those who were part of its formation, meaning our findings may be coloured by personal opinions of the set of people we spoke to, however neutral they expressed themselves. Some actors within the government may therefore be underrepresented in our interviews. We did not speak to the Ministry of the Interior and Kingdom relations (which also includes the Dutch General Intelligence and Security Service (the Algemene Inlichtingen- en Veiligheidsdienst, or AIVD)). Likewise, the Ministry of Foreign Affairs was not spoken to, while they will definitely encounter results of the Dutch position in international contacts. Whilst the political party backgrounds of the people we spoke to is likely to differ, our view on the parliamentary angle is limited as we spoke to a representative of just one party in that context. While we did employ results of interviews in other interviews we did not do systematic fact checking

In the end our thesis tries to find insights into the way we can analyse positions of political actors in the encryption debate and into the process that led to the formation of the Dutch position on encryption. Our thesis does not form an opinion on what that position should be, so limitations in the widths of opinion expressed by the people we interviewed should be of limited effect. However, the

end result is that our thesis cannot and will not presume to leave no stone unturned, meaning some of our conclusions should be treated as preliminary.

At times the conversations with our interview subjects and our research into literary and media sources felt close to investigative journalism. However much this has its own merits, we feel the judgement of the value of individual expressions, the limitations to our approach as we have mentioned them in this chapter and the basis of literary review firmly put us in the territory of academia.

The debate on encryption is International in its nature, in light of our research questions we have regularly applied focus on the Dutch debate, laws and regulations.

IV. A primer on encryption in communications

First things first: what is a backdoor? Definition of the concept is not part of this thesis, we will work from the following definition, based on a definition by the US Electronic Frontier Foundation (Schoen 2016) and the concept's entry in the Oxford dictionaries[8]: a backdoor is any (possibly secret) feature or defect of a system that is used to circumvent normal security checks, allowing surreptitious unauthorised access. A backdoor does not necessitate it being result of government regulation, though that is the form that is specifically of interest for our research questions.

Historically, in Information Technology, the concept of a backdoor shows up somewhere in the eighties of the previous century[9], having been used for the bypassing of normal authentication in systems for reasons varying from dealing with lost passwords to implicitly or explicitly gaining access to encrypted communications.

A backdoor can be many things and need not be limited to an IT environment. A master key to a set of locks is essentially a backdoor, a system with a built-in emergency access account with a default password is a backdoor and a cryptographic key that will allow decryption of information, even if a sender and receiver of a message used a different key to secure their message, is also a backdoor.

I. A short history of encryption backdoors

As long as people have been communicating there has been a drive to keep those communications secret from other people, be it for reasons of social group security, the protection of trade secrets or simply reasons of privacy. Ultimately this results in encryption not being a new technology and the concept of backdoors being, quite literally as we shall see further on in this paragraph, as old as the way to Rome.

Ancient beginnings

Any class on encryption starts with examples from the past, notably the cyphers devised by the Romans (Yaschenko 2002, 141) and Greeks (Yaschenko 2002, 154) , though Mesopotamian encryption predates even that, in the form of an encrypted cuneiform tablet from 1500 B.C.E. (Grossman, Lo, and Schmetterling 2006). With the desire of people to keep their information secret came the insistence of other people to still want to know what this secret information was. An early example that relates to this are the Agentes In Rebus, probably instated by Roman Emperor Diocletian, who formed a form of government messaging service, including a special type of agent

[8] https://en.oxforddictionaries.com/definition/back_door

[9] The notion of a trapdoor surfaced in a 1967 paper, but this term has been used for cryptographic functions that are easy in one direction but hard to reverse since the 1970's, leading to use of the term backdoor. See [8].

called the Curiosi who had secret agent like roles to be able to know contents of communications (Kazhdan 1991, 37). These were of course times when government (with less democratic sense than in today's world) often had a more absolute power over a nation's inhabitants, meaning discussion on moral or ethical grounds of the impact of this intrusion on one's personal life did not lead to public debate.[10]

Secrecy of correspondence

Postal services are old, the desire to know what other people are talking about through the mail is, like the earlier reference to the Roman empire shows, equally old. Looking into the Dutch legal framework surrounding this, we learn that letters may not be opened before they reach their destination, unless a judge has ruled this as a necessity for one of the allowed forms of investigation (Grondwet 2016, article 13). These allowed forms vary from criminal investigations by police services and Public prosecutors to activities by Civil and Military intelligence services.

Though the access to postal correspondence makes for an interesting comparison, there is a problem with this parallel: postal messages have no built-in encryption. The state of a letter of being closed is unequal to an encrypted bit of digital information. Though various forms of protection for contents sent through the mail exist they usually take the form of insurance and rarely of physical protection. Opening of an encrypted message necessitates a cryptographic key, opening of a closed letter necessitates a letter opener, or perhaps just one's hands. However, when people communicate with each other via post they can arrange any form of encryption they like for the contents of their messages, taking it outside of the normal reach of capture, unless an agent, having captured a postal message with some form of cypher, then starts trying to decrypt things. There has never been regulation that forbids persons from sending messages in code, making it at least questionable why some governments think the digital world is so different that they are trying to get it instated there.

In conclusion, the postal situation is quite comparable to the situation of digital communications: an encrypted digital message cannot be read when it is received without the proper cryptographic key, just like a letter between two people who agreed upon some cypher beforehand cannot be read by the holder.

WWII and Cold War era

When encryption is discussed the use of the Enigma system by the Germans in WWII is oft used as an example. The breaking of this cypher, an important step for the Allies, was made possible not by a backdoor but by using a so called 'known-plaintext' (Gaj and Orlowski 2003, 115) attack. Governments on the allied side were, however, actively seeking out the help of manufacturers of parts of the machine, which did not result in an actual backdoor being placed in it but did give them insight into who used which parts. The BBC, in an effort of sifting through declassified NSA documents were able to determine that, in the post WWII Cold War era, a Swiss manufacturer of encryption machines helped "keeping the NSA and GCHQ informed about the technical specifications of different machines and which countries were buying which ones" (Corera 2015).

The time also saw extensive regulations controlling the export of technology from Western countries to other countries. Trade limitations were mainly aimed at military supplies and since the use of encryption was mainly used for military purposes it became part of these limitations. Export was possible but only with an export licence, which came under growing demand as the financial sector, due to growth in the money transfer market, started to require strong encryption.

[10] This is speculation on our side, no research was done into the political side of debates on (backdoors in) encryption before the 1990's.

In the 1970's Whitfield Diffie and Martin Hellman published a paper on what would ultimately become the basis of much of today's cyber security: Public Key Cryptography. In their paper they showed a method, using a Public key made known to the world and a Private key kept to oneself that allowed individuals to communicate securely without the need of some other method to share an encryption key that needed to remain secret (Diffie and Hellman 1976). Building on Diffie and Hellman's ideas, a trio of scientists (Ronald Rivest, Adi Shamir, and Leonard Adleman) developed an actual system that applied this type of encryption. These developments, predating the 'Crypto Wars' of the nineties, started actions from some factions in the US Government to dampen cryptographic developments. Cryptography was increasingly seen as a threat to security (Levy 2001).

The eighties also saw its share of discussion, though apparently somewhat distanced from the general public. Debates about export of encryption in the nineties (see the next section for more on that) saw mention of a "*row between the NATO signals agencies in the mid 1980's over whether GSM encryption should be strong or not*" (R. Anderson 1994) which was further unearthed when a Norwegian paper spoke to several experts who recalled discussions for a weaker encryption key, mainly pushed by the British (Faeraas 2014). In the end this culminated in a compromise which effectively left the encryption used for the GSM system for mobile phones with a 54-bit key[11], and not the proposed 128-bit variant (Ibid.).

Phone encryption: the Clipper era

While, as we have seen, governments' wishes to access encrypted data had long existed, this did not lead to much public debate before. This changed in the 1990's when the US Government was confronted with the addition of communication encryption to mobile phones. The debates, hearings and other proceedings surrounding this period have been dubbed the 'Crypto Wars', and are currently oft referred to as the 'first' 'Crypto Wars', as we find ourselves in the middle of the second 'Crypto Wars', which is, interestingly enough, again mostly triggered by the usage of mobile phones, albeit for the usage of communication applications using the Internet, and not strictly for voice communications.

The setting of these first 'Crypto Wars' was much the same as nowadays: government agencies were increasingly worried about secret communications between criminals and terrorists that, when intercepted, were no longer usable: wire taps lost their function for the contents of communications. This 'going dark' because of built in encryption of voice communications in mobile phones led the NSA to design the so called 'Clipper chip' (Gallagher 2015). This government designed chip would be mandated to be inserted into consumer phones, both supplying them with cryptographic services and allowing the method used for this to have a built in channel through which intelligence agencies and law enforcement could still decrypt communications when deemed necessary (Kehl, Wilson, and Bankston 2015, 5).

After proposals for insertion of the Clipper chip in phones was announced a hitherto unseen coordinated protest started, bringing together cryptography experts, civil rights organisations, hackers and industry leaders (Diffie and Landau 2007, 236).

Despite this the government pushed forward, engaging the opposition from technologists in an article in Wired entitled "Don't Worry Be Happy" in which the then Chief counsel for the NSA points out why they feel Clipper was necessary. Ultimately this was not successful (and one can wonder why it was thought that statements like "*We can't afford as a society to protect pedophiles [sic] and*

[11] With computational difficulties for the cracking of keys generally increasing when keys become larger (more bits) this essentially made cracking of these keys in cellular networks easier.

criminals today just to keep alive the far-fetched notion that some future tyrant will be brought down by guerrillas wearing bandoleers and pocket protectors and sending PGP-encrypted messages to each other across cyberspace" (S. A. Baker 1994) would be helpful. The discussion raged on for a while but the Clipper chip plans were ultimately scrapped. From a technical point of view serious flaws were found in the way the Clipper chip did its work, showing that it could be circumvented (Blaze 1994). On the other side there was also opposition to the proposal from a business point of view: if consumers or businesses are faced with a choice between buying a US encryption product with a government mandated backdoor add-on or a product from another country that does not have this backdoor (of which there are many) they are likely to choose the non-backdoored version anyway (Kehl, Wilson, and Bankston 2015).

The debates surrounding the Clipper chip contain much similarities with the current situation. Next to inherent technical problems in backdoor access, and the privacy impact of special access, the state of a nation's economy is apparently an influence on the decision making of politicians, albeit only after substantial discussion.

Transport security (a brief detour into travel locks)

Stepping out of the communication domain we can see other, physical, situations where the concept of backdoors plays a role. Next to long known concepts of skeleton keys for door locks a more comparable (and fairly recent) analogous concept is formed by airport security access to luggage. While this seems a far-fetched comparison at first sight, a closer inspection reveals similarities that explain why this example made its way into the debate around government sanctioned circumvention of encryption: it illustrates the fragility of any backdoor (Schneier 2015). Here we see an example of a regulatorily mandated access method that circumvents the actual owner of lock and key: an example of public rules and regulations[12] that provide access to information (luggage contents) that would otherwise be locked away.

In essence the situation is thus: US air travel regulations and treaties define rules about the inspection of luggage. These are defined by the Transport Security Administration (TSA), an agency which is part of the US Department of Homeland Security. Essentially these regulations come down to inspection of luggage being done regardless of what locks travellers put on their luggage, but using specific locks will mean these will not be broken off (essentially a brute-force attack against encryption of a suitcase). While this isn't much of a security measure per se (a simple set of wire cutters can easily circumvent it), the regulation[13] surrounding approved locks is what makes it interesting for this comparison. The specific locks in question are allowed because TSA approved locks have a backdoor, in the form of a standard set of keys that airport security personnel can use to gain access without damaging the lock.

Here we see a fitting comparison between the backdoors on encryption in cyber space and backdoors in the real world. A form of lock is used to protect a form of content, but the lock in question has a built-in way of allowing third parties access without knowledge of the actual owner of the content.

What makes this parallel specifically interesting is the fact that a blueprint to this backdoor became public. This was not intentional, neither was there a leak or hack but rather a case of naivety through which the TSA master key set became public: a photograph in a news article(Halsey 2014) showed a

[12] Primarily based on the US TSA rules.

[13] Which is hard to find in detail, TSA states little that can be seen as a direct source ("Travel Tips | Transportation Security Administration" 2016). One of the makers of TSA approved locks has some more information to share. (Travel Sentry 2016)

picture of the keys that was sufficiently detailed to allow a clever reverse-engineer to 3d print his own set of TSA backdoor keys (Greenberg 2015).

Brute forcing a lock to get into someone's luggage would be easily done with a sturdy screwdriver, much less effort than the brute force needed to break an AES (Arora 2012) encrypted password that protects an encrypted hard drive. However, the point here is that the cyber domain is not alone in its problems, risks and debates surrounding lawful access by government sanctioned parties.

Concluding

To be sure both encryption, backdoors circumventing that encryption and government endeavours to gain the edge against parties applying encryption is not new. Public criticism and debate of such efforts do seem more recent, and still seem to be growing. We will encounter more of this in our analysis of the current debate in the next section.

II. Current debate

In both the US and Europe a renewed discussion on the 'Going Dark' of intelligence services started with mobile phones found after criminal or terrorist activities. The US has seen a lively debate between the FBI and Apple about encryption (Farivar 2016), resulting in proposals for new laws in the Senate (Bennett 2016). In Europe the same debate gained traction after terrorist attacks in France, principally in the responses by then UK Prime Minister David Cameron (Gilbert 2015) and a later proposal by French and German Ministers for the Interior asking for laws that force Internet companies to decrypt data (Lomas 2016a).

The nature of this second instalment of the 'Crypto Wars' seems different to the Clipper era in several ways; Firstly it is much more global (the Clipper Chip discussions were in essence a US internal affair); Secondly the general public has shown more concern (possibly due to the ubiquity of voice and messaging applications that include encryption (perhaps combined with a growing sense of loss of privacy in the current social media age).

Different nations have differing views on this debate. Most understand the challenges that police and intelligence services face in fulfilling their tasks in a world which sees communications being encrypted more and more. Yet the tender balance (or perhaps more correctly: trade-off? (Hildebrandt 2013)) between privacy and security is as much part of the debate as in earlier instalments.

Before we can state anything about the nascence of the Dutch Cabinet position on encryption and generalisable success factors that could be applicable to other countries we need to better understand the more global nation of the current debate.

To present an overview of current national opinions in this debate we have done a brief analysis of public sources that voice governments' opinions. We present this as an overview of countries official positions on encryption (or what officious positions seems to be where an official position is not present). This overview was created without in depth research, based mostly on sources readily available on the Internet. Per country we have included information on local debates on encryption and a brief analysis of what their viewpoint seems to be based on.

The group of selected countries may seem random, it is based on those countries that either responded to an EU meeting in which a questionnaire was given to member states about how often they ran into encryption from a law enforcement point of view (Council of the EU 2016), were mentioned in a Law Library of congress investigation into the subject of government possibilities

surrounding encryption (The Law Library of Congress 2016) or were prevalent in the media due to discussions or statements about encryption.

That not a lot can be found about country's official position within this debate hardly comes as a surprise. Governments and their rules and regulations move on a slower timescale than Internet developments. A 2013 study of a group of national cyber security strategies reveals large differences between the level of maturity in these strategies that countries have achieved. (Luiijf, Besseling, and Graaf 2013). If some countries have only recently come to grips with the presentation of a cyber security strategy the fact that there is no statement or position on encryption as used in communication channels like WhatsApp or Signal is unsurprising.

There is some existing research, though. As a part of his PhD research at the end of the nineties, Bert Jaap Koops looked into "The Crypto Controversy. A Key Conflict in the Information Society" (Koops 1999), which also resulted in a website tracking cryptography related laws of countries[14]. Much of the current debate is in a pre-law state, so none of it is reflected in the laws presented on this site. Tracking of developments stops in 2013, ending the overview before the current debate kicked off. More recent data can be found in a report (Freedom House 2016) from the Freedom House organisation[15], a watchdog organisation that promotes freedom and democracy globally, who did an extensive survey of Internet freedom worldwide, including information about if and how encryption is limited by asking *"Are there laws restricting the use of encryption and other security tools, or requiring that the government be given access to encryption keys and algorithms?"*(Freedom House 2016, 1019). However, there is little information about the debate behind it. In a web page dedicated to the report the following graph is presented, presenting us with an overview of countries where use of apps[16] is free or limited by government laws or regulations.

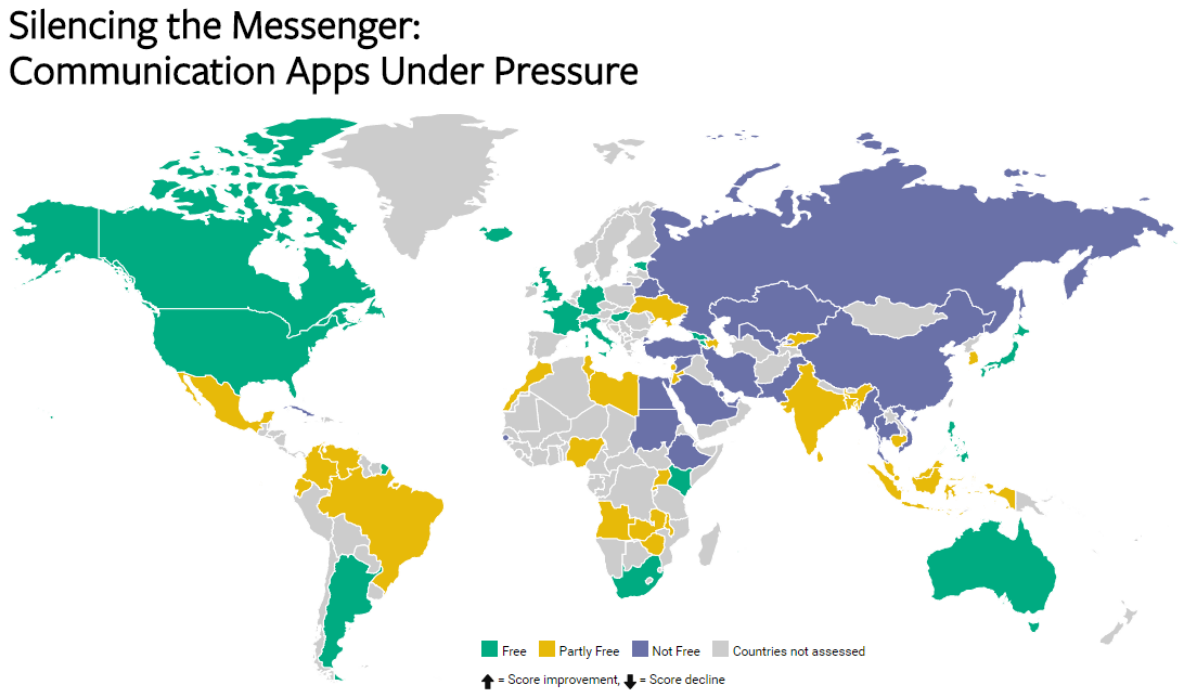

Figure 3: Freedom House's 2016 overview of app freedom. (Kelly et al. 2016)

[14] http://www.cryptolaw.org/
[15] https://freedomhouse.org/
[16] In the broadest sense, this is not limited to limitations in encryption but often about blocking apps altogether.

While there is a substantial set of information in the report we do see that the Netherlands is a country that was not assessed[17].

A brief word on our method: this chapter is called a 'quick scan' for a reason. Many reports (like the Freedom House one mentioned earlier) describe Internet freedoms in countries worldwide. We have not gone through all of these in detail, neither did we pursue in depth research of media in the countries mentioned to be sure of every last debate. The following chapter provides some background on the current debate based on information that is readily available. Countries that have been included are so due to lively local debates, noteworthy court cases or other factors that make them interesting as a backdrop for our later analysis. Countries are presented in alphabetical order.

Brazil

Perhaps an odd country to see mentioned in what is ultimately a case study of the Dutch situation, Brazil has seen its fair share of debate on encryption. Though more as an illustration of side-effects than anything else. The chat app WhatsApp has been blocked multiple times in Brazil, following court orders, after WhatsApp failed to cooperate with local courts (Leite 2016). While blocking applications in its entirety may (arguably) be better than undermining encryption by adding a backdoor or delivering keys to governments the result of this block was altogether different: people massively started using other (encrypted) messaging services (Cushing 2016), especially Telegram (Stone 2016).

Brazil's actions seem to stem from a national security angle, with companies being asked to aid the government, and non-compliance leading to either blockades or frozen bank accounts (Lomas 2016b). Brazil's high court has so far overturned all blockades due to violations to freedom of expression and communication (Agencia EFE 2016).

Canada

Canada entered the news surrounding the current debate when it became clear that Canadian police gained access to BlackBerry's global decryption key as far back as 2010 (Ling and Pearson 2016). Canada also has rules, as a part of the Solicitor General's Enforcement Standards (SGES) that implies that communications providers must retain decryption keys for communications they encrypt[18] (Parsons and Israel 2015).

A public debate challenging these government possibilities seems, strangely, not to have started, apparently due to a lack of transparency about the government's positions and policies (Braga 2016). The same article has the chairman of the committee on public safety and national security merely stating "*while encryption and backdoors are of great concern to a number of people, they have not yet surfaced as issues for our committee in its early days*"(Ibid.).

China

On a different end of the spectrum than many countries that operate in more democratic regimes China has quite a different position on encryption. Though argued from an economic point of view that promotes local industry and export "*China now insists that hardware and software made or used in China only employ cryptosystems developed in China*" (Swire and Ahmad 2012, 418) which naturally raises concerns over both the quality of this encryption and the presence of any backdoors mandated by the Chinese government. The nature of Chinese society means little public debate about this approach is visible, allowing the government to take this approach in their battle against

[17] Which is remarkable, as the Dutch Ministry of Foreign Affairs is named as one of the supporters on the index page.

[18] Which is notably different from encryption provided by a chat app like Signal, where the encryption keys are essentially (automatically) created by the end user on their device.

'Going Dark' as opposed to contemplating mandatory backdoors (as seen in US/EU debates) or limiting the strength of encryption (the way India seems to be going (Prakash and Grewal 2015)).

There is quite a set of rules and regulations surrounding encryption companies should be aware of before starting their business in China (Bird 2016). While China does not have clear rules on encryption or backdoors, it has laws that state companies that employ encryption must first get a licence from the government. When a group of Chinese human rights activists apparently did not acquire (or did not receive) such a license but did start using Telegram that service saw a DDOS that took the service offline in Asia Pacific, a DDOS most probably originating in China (Horwitz 2016).

Debate is not common in China, which makes it noteworthy that Huawei, one of the large technology companies in China, seems to back Apple in its battle with the FBI (Reuters 2016). A spokesperson for the company stated "*Privacy protection is very important for Huawei, we put a lot of investment into privacy, and security protection is key, it is very important for the consumer*"(Ibid.).

China regularly pressures companies into complying to their strict censorship, most prominently by means of the great firewall of China, which is "*aimed at curtailing collective action by silencing comments that represent, reinforce, or spur social mobilization*" (King, Pan, and Roberts 2013). Though censorship has an indirect relation with encryption this does show a glimpse of an officious position that, backdoors or not, the government should have access to information. This is also expressed in a new law that, though it does not require backdoors, mandates companies to decrypt data when demanded (Moody 2015).

Overall China mainly makes it very clear control should be firmly in the hands of the government, mainly for national security reasons, while also aiming to boost China's own cryptographic sector by mandating products from China to employ Chinese built encryption.

Denmark

Denmark has previous experience with Internet privacy related laws and the difficulties they bring. A law demanding telecommunications providers to store their subscribers personal data for a year has (after five years) not led to any usable results for the police, while being disputed by privacy advocate and telecommunications providers alike (Olander 2013). So, Denmark has had some prior notice before engaging the current debate.

After analysis of the responses to the EU questionnaire we mentioned earlier (Council of the EU 2016), it appears that "*Authorities in Estonia, Denmark, Finland, Croatia, Italy, Poland and Sweden often come up against encrypted data during criminal investigations*" (Stupp 2016b). Denmark has taken steps that limit use of encryption to an extent, perhaps as a result to a long threat of terrorism, leading to an attack in 2015 (Brabant 2015). This has led to growing concern from digital rights defenders, especially since Danish law has some provisions on encryption: "*With regards to encrypted data, if a telecommunication provider has an integrated encrypted system, it must be sure to provide the police access to the data in a non-encrypted form*" (Privacy International and IT-Political Association of Denmark 2015, 6), this is nuanced by the added statement that "*If the data is encrypted by the customer's own systems, the telecommunication provider is not required to decrypt the data, as the comments of the Telecommunication Act note that this will be technically impossible. There is no key disclosure law requiring a suspect in a criminal case to release encryption keys or decrypt data*" (Ibid.). Which clearly opens the option of encryption to end users.

Denmark appears to be fighting for freedoms while at the same time encountering the threats some present in the light of other's freedoms, putting the country in the middle of the trade-off versus balance considerations we mentioned earlier in this paper.

Estonia

As it neighbours Russia and was once part of the Soviet Union, Estonia has seen its fair share of tension with its neighbour (Blomfield 2007), especially in the cyber context.

Estonian cyber security development has a lot of initiatives surrounding cryptographic technologies, through which each Estonian now holds a chip card for all government related business, which is also offered to the world for people wanting to become e-residents of the country (Prisco 2015). Also seen in the digitisation of all affairs citizens have with their government which has some publications declaring Estonia the (governmental) leader in secure digital authentication (L. Anderson 2015). To add to this, this Estonian ID card, used for many government interactions has no back door, as the former premier of Estonia (and currently works for the European Commission) states "*I am strongly against any backdoor to encrypted systems*" (Valero 2016), explaining further: "*In Estonia, for example, we have an e-voting system. If people trust an e-banking system, they can also trust an e-voting system. This trust is based on a strong single digital identity guaranteed by the government, which is based on encryption. The question is who will trust this e-voting system if there are some back doors and someone has the keys to manipulate the results. The same goes for the e-banking system*" (Ibid.).

As was mentioned before, Estonia was one of the countries responding to a EU questionnaire stating they "*often come up against encrypted data during criminal investigations*" (Stupp 2016b) though this has not led to any wishes to gain better access to encrypted data in Estonia, quite to the contrary as a report found their national ombudsman, in 2015, "*playing an increasingly active role in supporting privacy rights related to digital data and communications*" (Freedom House 2015), in addition to the statements Estonia's former premier made.

Estonia seems to have put citizen's security on their agenda as a high priority item, also seeing a secure digital economy as an advantage over other nations.

EU as a whole

The EU as such expresses a lot of opinions through its various committees, organisations, working groups et cetera. A singular European statement on the subject of backdoors is not present. The overall summary the American Law Library of Congress states about the EU: "*At the European Union (EU) level, there is no requirement that keys to encrypted materials be disclosed to law enforcement authorities, or that companies decrypt communications in response to a government request. … In a similar vein, the EU's law enforcement agency, Europol, favors [sic] enacting legislation on disclosure as the only practical solution for handling encryption when the keys are held by individual users*" (The Law Library of Congress 2016, 27), without any specific EU laws or guidance, dealing with encryption is put in the control of individual member states.

The European Union Agency for Network and Information (ENISA), the EU's cyber security agency, opposes backdoors (Stupp 2016a), with the ENISA director being particularly vocal about this, stating: "*If you have a potential backdoor in an encryption implementation, then the question is, how can you [ensure] that terrorists or criminals don't attack it and don't use it?*" (Geller 2016).

The aforementioned former Estonian Prime Minister Ansip, in his role as European Commission Vice President for digital markets also stated there are no plans to require backdoors in encryption, in Europe, stating "*In the European Commission we never had, and we don't have, any kind of plans to*

create back doors" (Eckstein 2015). Reports from the European Data Protection Supervisor hint at revised privacy laws banning encryption backdoors altogether (Buttarelli 2016).

The information present points towards wide support of strong encryption, for various reasons, from the EU itself, though specific legislation remains a function of member states.

Finland

In the EU questionnaire on encryption Finland also responded, noting that they do regularly encounter encrypted data in criminal investigations. That seems about the extent of Finnish involvement in the current debate, not a lot of information shows up through Internet searches.

Finland does have laws that address encryption "*The Privacy and Data Security in Telecommunications Act of June 1999 (no. 565-1999) allow telecoms users and subscribers "right to code their telecommunications message in the way they wish utilising the technical possibilities available thereto". Telecom operators have to inform users about the possibilities to protect communications.*"(Koops 2013). The same source also mentions that, in the Clipper era, "*At the OECD meeting of December 1995, Finland did not approve key escrow proposals. The chairman of the Finnish public administration's group for data security affirmed that Finland will not require key escrow*." (Ibid.).

Research into the Finnish position delivers a lot of legislation that is, in relation to the current debate, quite old but still very relevant. This seems to suggest the laws mentioned above will still be in place, especially as recently the Finnish Communications Regulatory Authority granted approval for a smartphone that aims to provide secure communications (elisa.com 2016).

Overall Finland seems to support privacy and the end user's freedom to choose whichever way they want to secure their communications.

France

The Charlie Hebdo attack in the beginning of January 2015 (BBC 2015a), together with the attacks of November of the same year (BBC 2015b), again targeting Paris, seem to have propelled the debate on encryption back to the forefront of political agendas. Perhaps understandable, had the attackers used encrypted means to communicate, but this appears not to have been the case (Bode 2015), in particular for the attackers of the Bataclan concert hall, as noted in this excerpt from The Intercept on the matter: "*European media outlets are reporting that the location of a raid conducted on a suspected safe house Wednesday morning was extracted from a cellphone [sic], apparently belonging to one of the attackers, found in the trash outside the Bataclan concert hall massacre. Le Monde reported that investigators were able to access the data on the phone, including a detailed map of the concert hall and an SMS messaging saying "we're off; we're starting." Police were also able to trace the phone's movements*" (Froomkin 2015).

France is arguably the place where the current instalment of the debate surrounding backdoors started. It saw more than a fair share of terrorist attacks, perhaps resulting in the firmer political demand for access to encrypted data when compared to most (at least European) other nations.

The French Interior Minister wants a global initiative to tackle the problems encountered due to encryption, and planned talks with his German counterpart, stating "*Messaging encryption, widely used by Islamist extremists to plan attacks, needs to be fought at international level*" (Masnick 2016a). Earlier in 2016 French Parliament voted in favour of fines for technology companies that do not cooperate fully in investigations to do with terrorism (France-Presse 2016). France has probably not seen the end of this debate yet, though the climate already seems a bit more nuanced than at

the start of 2016 when the French Government contemplated laws that would outlaw strong encryption altogether (Howell O'Neill 2016b). Other opinions do exist in the French Government, as the "French Secretary of State Says Encryption Backdoors Are 'Not the Right Solution'"(Howell O'Neill 2016c)(Thomson 2016), but they seem to be a minority.

Overall France, probably triggered by the string of terrorist attacks, is mostly on the path towards greater possibilities for investigative agencies to have lawful access.

Germany

Following the first set of terrorist attacks in France, early in 2015, while many countries expressed outrage and called for more government access to encrypted information, Germany initially took a step in the other direction, stating in their digital agenda "We *support the use of more and better encryption and aim to be the world's leading country in this area. To achieve this goal, the encryption of private communication must be adopted as standard across the board*" (Zaske 2015).

But in august of 2016 Germany joined France in proposing legislation that would force companies like WhatsApp and Telegram to unlock encrypted messages, as we mentioned before in the paragraph on France.

Strangely though, the proposal by France and Germany seems to want both backdoors and strong encryption, stating in their proposal both that "*The principle of encryption … should not be called into question*" (Ministere de L'Interieure 2016)[19] but also "*… this would mean requiring non-cooperative operators to remove illegal content or to decipher messages in the course of investigations*" (Ibid.)[20] which, while being sarcastically reported on by some news outlets to be akin to wanting "*A and not-A at the same time*" (Falkvinge 2016), may be on the right track if considered with a little more distance: a method of encryption that would be strong and secure for all users but would still allow lawful access to investigative agencies in individual cases (thus not hurting the privacy of non-suspects) may be too much to ask from a technological viewpoint, but it does address the needs.

Hungary

Hungary is, together with Italy, Latvia, Poland and Croatia, among a group of countries within the EU who want new legislation that allows police forces to better deal with encryption (Reback 2016).

Hungary has taken a lot of steps on this subject already, which for all intents and purposes makes quite clear that they value national security greatly. Law proposals from Hungary, made reportedly to be able to cope with terrorist threats, vary from banning encryption software altogether to mandating telecommunication companies to store data of encryption users, whilst providing maximum privacy from state owned companies, protecting these from public scrutiny (EDRi 2016).

Laws that would target citizens using encryption were also proposed but ultimately not created "*One of the most controversial proposals would have given the government the right to sentence anyone who uses an app to ensure the secrecy/privacy of smart phone conversations. From the little we learned from the generally upbeat descriptions of the meeting by opposition politicians, they managed to convince the government that only the manufacturers of such software would be criminally liable*" (Hungarian Spectrum 2016).

Within the EU Hungary seems to have followed the fastest path from government ideas about access to encryption to actual legal proposals, though many proposals have not passed parliament. Their response in the EU Council questionnaire on the subject reports that they rarely encounter

[19] Original text in French, translation aided by Google Translate.
[20] Original text in French, translation aided by Google Translate.

encryption in the course of criminal procedures, that there are no laws for citizens or companies to provide encryption keys but that it is possible to intercept encrypted dataflows though the unit involved does not deal with decryption of this data (Council of the EU 2016).

The Netherlands

When searching for information on the Dutch Government and its reaction to the encryption debate the first thing encountered is the Dutch Cabinet position on encryption which, after looking at different societal interests ultimately concludes: "*The cabinet is therefore of the opinion that at this point in time it is not desirable to take restrictive legal measures as regards the development, availability and use of encryption in the Netherlands*" (G. A. van der Steur and Kamp 2016).

This is not the end of the debate in the Netherlands, though, as several discussions have sprung up after publication of the government position. The head of the Dutch intelligence services presented a different vision, taking a position that opposes the country's official statement[21] (J. Baker 2016). The Dutch public prosecution office also expressed wishes to access encrypted information (Schellevis 2016). Both cases were discussed in parliament, with the responsible ministers restating the Cabinet position.

More recent developments in the Dutch case were not about encryption per se but about the government's possibilities of hacking into individual devices, a need expressed by the national coordinator for anti-terrorism (Hendrikman 2016). This approach was received as more understandable by notable opponents of weakening encryption, Dutch digital rights defender Bits of Freedom, who see hacking attempts as part of an intelligence services work but do wonder what the services will do with any vulnerabilities they find (Zenger 2016).

The Netherlands seems unique in that their government has published an official Cabinet position that endorses encryption. We will further investigate how this came to be in chapter VI.

Russia

Russia appears, perhaps unsurprisingly, to be in the select group of countries that address the encryption debate primarily from a government control angle (though usually under the guise of anti-terrorism measures). Some of the Russian statements seem doubtful however, like the KGB statement that they developed the ability to decrypt any encrypted Internet service (Moody 2016b). This follows an order from Russian president Putin to do so, for which he gave a timeline of two weeks (Masnick 2016b).

Russia's Parliament has also proposed laws that mandate messaging applications to build in backdoors to allow for government access, proposing fines for companies that do not comply. (Soeteman 2016). Further anti-terrorism laws also demand Russian ISP's to store content and metadata, despite protests from Russian ISP's that this is such a costly operation that none of them would be able to finance this endeavour (Moody 2016a).

Slovakia

2016 saw Slovakia take over presidency of the EU from the Netherlands. For the encryption debate their presidency mainly saw attention in the wish to discuss encryption with all the EU member states (Security.nl 2016). It is from this wish that the EU council questionnaire followed, though Slovakia itself seems not to have responded to it, at least not in a way that was published following

[21] The Dutch digital rights organisation Bits of Freedom responded by offering him a course in fundamental rights (van der Kroft 2016)

an information request from Dutch digital rights organisation Bits of Freedom (Council of the EU 2016).

United Kingdom

The UK has presented a strong reaction to terrorist attacks in France, perhaps stronger even than France itself. Former UK Prime Minister David Cameron, has stated: "*The question we must ask ourselves is whether, as technology develops, we are content to leave a safe space—a new means of communication—for terrorists to communicate with each other. My answer is no, we should not be"* (Bienkov 2015). Cameron seemed even to question whether any form of communication that is not readable by the government should be allowed to exist (Gilbert 2015), which comes across as somewhat uninformed not merely on the cryptographic level but also on the privacy level. This has sparked debate in the UK, and a response from media, some of whom sarcastically commented that David Cameron *"hasn't got a clue"* (Ball 2015). The nation's intelligence service, GCHQ, seems to have a differing opinion as its director spoke out against weakening end-to-end encryption or the addition of backdoors (Weitzner 2016).

In the response the UK gave to the EU council questionnaire on the subject, they remarked that their law enforcement authorities "*almost always*" encounter encryption in the course of criminal procedures, that there is an obligation for suspects to give up encryption keys and passwords when asked but responded that there are no laws requiring ISP's to do the same, or laws that allow interception of encrypted data that is then decrypted (Council of the EU 2016).

The most recent development in the UK was the signing into law of the Investigatory Powers Act by Prime Minister May, a law which, on closer inspection seems to include wording that can be interpreted to oblige removal of protection by operators (McCarthy 2016). Though May, in the role of Home Secretary had earlier stated that encryption would not be banned. This legislation is rather recent, 2017 is bound to see more developments in the UK about what it entails exactly.

United Nations

The United Nations (UN), much like the European Union (EU), supports strong encryption and urges developments towards it. A special rapporteur for the UN Human Rights Council concluded in a report in 2015: "*encryption and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection*" (Kaye 2015). Which saw a response from human rights and media freedom organisations, urging all governments to adopt its recommendations (Human Rights Watch 2015).

Following the FBI versus Apple debate the human rights authority at the United Nations backed Apple's position in march of 2016, echoing the report of the previous year (Berman 2016).

United States of America

The US, as the originating country for the first 'Crypto Wars' of the 1990's, is again the scene for many a discussion on encryption.

The most widely publicised event is the battle between Apple and the FBI, which ultimate was not about unlocking of a single phone but the wish of the FBI to gain a software tool that would allow them access to any iPhone in their possession (Zetter 2016). The battle ended when the FBI withdrew the request, stating a third party helped them unlock the phone. When the matter was further discussed with US President Obama he presented a view much in line with the proposal to the EU by France and Germany, wishing for a solution that would both provide robust encryption and secure third party options to decrypt, stating "*You cannot take an absolutist view on this. If your view is strong encryption no matter what and we can and should create black boxes, that does not strike the*

balance that we've lived with for 200 or 300 years. And it's fetishizing our phones above every other value. That can't be the right answer" (Machkovech 2016).

US senators Burr and Feinstein presented a bill that included requirements for legislation to demand that services backdoor their decryption, sparking many a media story: Techcrunch reported on its scariness (Conger 2016), Wired declared it "Ludicrous, dangerous, technically illiterate" (Greenberg 2016b), while Quartz found it "Everything wrong with tech politics" (Gassee 2016). The bill seems to be off the agenda for 2016 (Reitman 2016), though we can but wonder what will happen to it if it resurfaces under the presidency of Trump.

The encryption working group of the US House Judiciary Committee, in their year-end report for 2016 stated "*That is why this can no longer be an isolated or binary debate. There is no 'us versus them,' or 'pro-encryption versus law enforcement.' This conversation implicates everyone and everything that depends on connected technologies—including our law enforcement and intelligence communities. This is a complex challenge that will take time, patience, and cooperation to resolve. The potential consequences of inaction—or overreaction—are too important to allow historical or ideological perspectives to stand in the way of progress*" (Encryption Working Group 2016), so developments in the US, as in many other countries, are likely to proceed at least into 2017. A year that will also see the instatement of a new US President: Trump.

Conclusion

Our quick scan shows that the position towards encryption varies with the background of specific speakers, the state of a nation's security seemingly relating to when they were last targeted by terrorist activities and the tools used by its adversaries.

Generically speaking we see three main categories of countries: those struggling with limitations to investigative possibilities (e.g. France, the UK, the US) those clearly stating strong encryption is a good thing (e.g. Estonia and the Netherlands) and those merely stating companies will need to comply with what the government needs (e.g. China, Russia).

Even when only looking at our quick scan of the current situation a few nations pop out as odd ones out, in a positive sense. Estonia has a clear anchoring of use of encryption in its legal frameworks but one nation has gone even farther, with the debate resulting in an official government position on encryption: the Netherlands. Why it is that the Netherlands has come to an official statement about encryption and how this came into existence will be the subject of chapter VI. But first we will devise a way to look at the debate from different angles, with the goal of opening up our view to as much understanding of the debate as possible.

V. Viewpoints on encryption

As we have seen in the previous chapter the assessment of the impact of encryption varies between different governments. Before we commence our case study of the situation in the Netherlands and the formation of the Dutch Cabinet position on encryption, we will analyse different possible viewpoints towards encryption.

We will do this by applying different possible viewpoints as possible lenses through which to view current events. For this, as we described as part of our chapter on methodology, we take inspiration from Graham Allison's analysis of the Cuban missile crisis in the 1960's. Allison determined different conceptual models with which to analyse the events surrounding the Cuban missile crisis.(Allison 1969). In Allison's case this opened up a new way of understanding actions and viewpoints of

political actors.[22] He showed that a strictly rational view that we may expect (or perhaps expect too much as researchers) does not explain all actions of those who are part of a debate, but if we consider an actor's backgrounds and the ways public administration work we can understand behaviour better and to a fuller extent.

Allison briefly explained his conceptual models by using the metaphor of a game of chess:

The rational actor model (I) which shows: "*that an individual chess player was moving the pieces with reference to plans and maneuvers [sic] toward the goal of winning the game*" (Allison 1969, 691).

An organisational process model (II) that shows: "*that the chess player was not a single individual but rather a loose alliance of semi-independent organizations, each of which moved its set of pieces according to standard operating procedures*" (Ibid.).

A governmental politics model (III) that: "*would suggest to an observer that a number of distinct players, with distinct objectives but shared power over the pieces, were determining the moves as the resultant of collegial bargaining*" (Ibid.).

He ultimately concluded that when applying a rational actor model people apply unreliable assumptions to an analysis, which in the case of actual crisis can have far reaching consequences. The key thing to take away from this in relation to our own research is that analysis solely based on rational actor models can be too limited and may not always help understand the full picture, the exploration of different viewpoints will help understand the bigger picture.

For our case study of the Dutch situation we will primarily base our observations on interviews with the group of people we described in our methodological section. Analysis of the output of these interviews from a rational (Allison's model I) point of view is surely possible. Determining what organisational process (model II) factors are in play is more difficult, due to the small set of individuals we interviewed. How much of what is said is a result of governmental politics (model III) is something we will not try to determine, both as we do not feel equipped to judge our interviewees' personal motivations and due to responses in our interviews generally seeming to stay away from the politics behind them. While doing this, we will keep in mind that the debate surrounding backdoors is very much political. Truly, the media outings of some countries politicians that we've seen in chapter IV may lead us to conclude that, indeed *"Politicians in democratic systems generally worry first and foremost about getting elected"* (Pierson 1996, 149). But we will not evaluate this any further.

This leaves us, when regarding Allison's models, with a heavy emphasis on his model I: rational actors. To alleviate this, we will build further on the notion that different actors will look at the same situation from differing backgrounds, leading to different (rational) conclusions of what is the right direction to move in. We will do this by superimposing an additional set of lenses to Allison' rational actor model (his model I). For our analysis of the current 'Crypto Wars' (specifically the debate surrounding backdoors in encryption) we will look at governments rational actions by applying the following three lenses: 1) An economic lens 2) a national security lens 3) a privacy lens. When looking through our own lenses the positions of different actors are expected to display elements of all three of our lenses, in varying shades.

[22] This method also helps a researcher to put some distance between his or her own opinions and the subject at hand, opening a path to the differing ways in which information can be analysed.

The choice of these particular lenses is not a chance happening. Both the historical background in chapter IV and our quick scan of the current debate in the last part of that chapter show these three angles represented by various stakeholders in the debate. The next chapter see both the Dutch Cabinet position and our interviewees refer to concepts that fit these three lenses. Literature on governance concerning Internet security also remarks that actors using the same vocabulary to explain their goals may very well disagree on the meaning of the vocabulary and thus the way to achieve these goals. As this conclusion from an article on security in Internet governance debates states: "*Government stakeholders advocate for limitations on WHOIS privacy/proxy services in order to aid law enforcement and protect their citizens from crime and fraud. Civil society stakeholders advocate against those limitations in order to aid activists and minorities and protect those online users from harassment. Both sides would claim that their position promotes a more secure internet and a more secure society—and in a sense, both would be right, except that each promotes a differently secure internet and society, protecting different classes of people and behaviour from different threats*" (Wolff 2016, 10). A conclusion which primarily hints at a split in considerations between national security and privacy (individual security). Based on findings from our earlier chapters and later interviews we have also incorporated the economic angle.

In essence we take from Allison that which Bendor and Hammond concluded in their 'Rethinking' of Allison's models where they stated that Allison in "*Essence of Decision made a persuasive case for the use of formal reasoning, for the development of alternative models to explain an important event, for the derivation of testable propositions from the models, and for the testing of the propositions."* (Bendor and Hammond 1992, 318) Though we will not derive (testable) propositions from our current analysis, leaving that an avenue open to future work. The rest of our analysis is based on Allison's model I (and the addition of our lenses) though we will see some elements of model II: organisational process and model III: governmental politics.

I. The economic lens

Companies, and the economy they operate in, are governed by rules and regulations of the countries they operate from and the countries they deliver their services in. The result of this is that a change in these rules and regulations will influence their bottom line, be it positive or negative. If this becomes enough of an effect it will have an impact on a country's economy as a whole. A company's customers mostly determine the services that they offer and it is ultimately these customers (end consumers and business to business) that have a demand for encryption.

The effects of legislation surrounding encryption will have effects on countries that is tied with their dependence on encryption as a technology. Thus, we expect this to be more of an effect in countries that have large (tele)communications, Internet, and hosting services.

It is these notions that our economic lens, as an extension to Allison's model I, is based on. If one analyses the debate surrounding encryption rationally, but from an economic angle, what then are the factors that will influence our judgement the most.

Effects of encryption

Encryption is a technology that forms the base of much of the trust in today's economic contracts. Online banking would not have taken off if communications between customers and banks would have been easily manipulated. In a 2015 research paper researchers from the Niskanen Center[23] concluded, after analysis of growth in economic sectors dependent on it, that "*it is clear that there*

[23] A libertarian think tank, so we must assume their report is at least somewhat biased, however the point they make supports the economic lens through which to study encryption.

are immense, semi-quantifiable benefits to be attributed to the proliferation of strong and easily accessible cryptographic protocols"(Hagemann and Hampson 2015, 24). Likewise, DIGITALEUROPE[24], a European organisation representing the digital technology industry, presented several actions policy makers in the field of encryption should focus on, including "*Promoting data security and privacy - Encryption is fundamental for the economic growth and societal enhancement of the data economy as it allows citizens and organisations to communicate and store information securely and confidentially while protecting data against increasingly sophisticated cyberattacks.*" and "*Avoiding technology mandates and backdoors - Government mandates on the design of technology including the creation of backdoors will impede innovation, hurt the economy, and weaken data security and privacy. Technology providers should be enabled to develop and implement encryption solutions tailored to achieve the best possible data security and privacy*" (DIGITALEUROPE 2016, 1). The more globally oriented organisation ITIF[25] comes to comparable recommendations, stating in a 2016 report that "*ITIF believes that the U.S. government should not restrict or weaken encryption, because any attempts to do so would reduce the overall security of law-abiding citizens and businesses, make it more difficult for U.S. companies to compete in global markets, and limit advancements in information security. Moreover, attempts to restrict or weaken encryption would be ineffective at keeping this technology out of the hands of many criminals and terrorists*" (Castro and Mcquinn 2016).

From an economic point of view there seem to be great benefits in unhindered encryption.

Effects of government backdoors

From an economic point of view, government sanctioned backdoors, by laws forbidding non-circumventable encryption or prescribing what encryption protocols must be used, present several problems. Much like the Internet has globalised communications is has also globalised trade, allowing consumers to pick and choose both their digital (email, storage, video) and physical (books, shoes and other supplies) outlets. Trust is an important factor for consumers when deciding where to purchase their goods, (Gefen 2000) and it is to be expected that a legal climate which undermines this trust (by mandating cryptographic standards that contain backdoors) will have an effect of the likeliness of consumers to choose a business operating in that climate. When consumers are expected to lose trust, this hurts businesses, leading to a key point of our economic lens: companies see countries with a high amount of regulation on their internet services as a disadvantage, which may lead them to base their companies elsewhere. The fact that EU law has certain privacy demands that cannot be met if a service provider bases its platform in the US can serve as an example in this: both Google and Microsoft started offering services to European customers from data centres within the EU as they would not have been able to provide their services to Europeans from a data centre in the US.

Another effect of government interference in encryption is that it would probably hurt those technological companies that provide encryption solutions in that government's country. There are many players in this sector, from a large number of countries, meaning alternatives are available to those who do not want to use an encryption product that may contain a backdoor. This means adding a backdoor to all encryption built within a certain country will have little effect on the possibilities of end-users that want to employ encryption. As research has *"identified 865 hardware or software products incorporating encryption from 55 different countries"* (Schneier and Seidel 2016) a fairly safe prediction is that the end user will be able to find another option. And this is merely a

[24] http://www.digitaleurope.org/About-Us
[25] https://itif.org/about

survey of available products, any criminal or terrorist organisation which is adequately funded will likely be able to have some IT department build their own.

In the clipper era, the article in Wired by the then Chief counsel of the NSA mentioned "*Key escrow will never work. Crooks won't use it if it's voluntary. There must be a secret plan to make key escrow encryption mandatory*" (S. A. Baker 1994) as a myth. This is not notable in itself, but one of the points in the explanation is relevant for the current discussion. The article mentioned "Encryption is available today. But it isn't easy for criminals to *use; especially in telecommunications. Why? Because as long as encryption is not standardized and ubiquitous, using encryption means buying and distributing expensive gear to all the key members of the conspiracy*" (S. A. Baker 1994) that encryption is standard and ubiquitous in the current age should need no further explanation, that this was thought in the 1990's was understandable albeit naïve but the point here is that not only crooks but any concerned company or individual has other options turning this myth into reality.

The first 'Crypto Wars' also saw argumentation along these lines, after the debate had run for a while economic implications gained visibility, becoming a factor for those in the political arena (Kehl, Wilson, and Bankston 2015, 13).

A third factor is formed by the cost of these provisions itself. In the circuit switched world of the past a wiretap was possible by copying a single signal to the relevant authorities. Building the same capability in today's Internet based environments means a telecommunications operator must be able to siphon out one user's traffic from a stream of millions and deliver the phone conversations therein to police investigators. Regulation that would mandate all encryption to have some form of backdoor for authorities will have a cost impact on those companies that are part of this encryption chain.

Bringing it all together: the economic lens

Since almost any type of regulation has an effect on a company's business operations, and therefore the economy as a whole a simple conclusion from an economic point of view is that less is more.

None but a very small section of companies that deliver information gathering services to a government can gain from any regulation diminishing the extent of encryption while many economic actors will suffer impact to their business when a government mandates certain implementations of encryption. To take this one step further: surely the economic climate of a country suffers when the economy is mandated to use only weakened forms of encryption when businesses in other countries do not face the same rules. Large corporations will simply take their business elsewhere and not settle in those countries that mandate backdoors in encryption.

Overall a viewer applying the economic lens to the encryption debate may not take a specific side in the security versus privacy trade-off but point more towards economic impact of far reaching regulation on this matter both in terms of direct costs and in terms of shifts towards products from different nations.

II. The national security lens

When viewed rationally from a (national) security point of view encryption appears as a double-edged sword. Encryption is both an asset, keeping correspondence between government agencies secret, and a threat, prohibiting examination of communications obtained in the course of work from police or intelligence agencies.

There seems to be an underlying scenario that keeps repeating itself: some international event shocks the world, (e.g. a terrorist attack or high-profile criminal case), following this government

politicians, tasked with the protection of national security, declare their inability to have prevented the event, and that it happened as a result of insufficient means for those agencies tasked with its prevention (most often the national police and (military) intelligence services). This is then followed by some form of proposal to expand the surveillance possibilities of the agencies tasked with prevention, which often includes a so-deemed necessity to be able to decrypt communications (most often presented as a need to gain access to information in mobile phones[26]).

For the current instalment of the 'Crypto Wars' the national security point of view has been voiced by spokespersons for various governments: as part of the 'going dark' debate in the US (Vance et al. 2015); former UK Prime Minister David Cameron also brought this up on various occasions (Bienkov 2015), and the Dutch Minister for the Interior Plasterk, together with his colleague Hennis-Plasschaert for the Ministry of Defence, also see a need for more powers for intelligence services, as requested in a new law (Pelgrim and Kas 2015).[27]

Effects of encryption

The threat against national security that encryption embodies is the largest effect of encryption that is visible from a national security point of view. While arguments exist (mostly from those more worried about privacy than national security) that strong encryption without backdoors is also to the benefit of national security this is not the point we will make here. If the dominant opinion from those who are responsible for national security would be that strong encryption benefits everyone the debate (and this thesis) would not exist.

The point has been argued many times, by representatives of many countries and more or less boils down to this: If criminals and terrorists have access to unbreakable encryption stopping their actions will become very hard. Privacy is recognised as a fundamental right so there is a wish to do all these things within the legal frameworks that already exist for wiretapping and searches through houses, when someone with the proper authority (be that a judge or high official in an intelligence service) deems removal of encryption necessary it will be done.

The effect of encryption without a means to bypass it, from the national security point of view, is that government agencies would "Go dark", and loose a significant method of gaining insight in criminal and terrorist activity. In a set of senate hearings in the US FBI Director James Comey explained the Going Dark problem as "*the growing challenges to public safety and national security that have eroded our ability to obtain electronic information and evidence pursuant to a court order or warrant*"(Comey and Yates 2015, 1). Stating later that "*The more we as a society rely on electronic devices to communicate and store information, the more likely it is that information that was once found in filing cabinets, letters, and photo albums will now be stored only in electronic form*"(Comey and Yates 2015, 3). The point being that encryption renders that information unreadable. A sentiment shared by other actors in the US investigative field, with a New York District Attorney reflecting on the inaccessibility of information, even after the correct warrants had been obtained, due to encryption policies of Apple and Google (Vance et al. 2015).

While we may indeed "*live in a "golden age for surveillance because investigatory agencies have unprecedented access to information about a suspect. In addition, data mining provides new tools for identifying suspects and their contacts. Law enforcement and national security agencies now have sophisticated data mining capabilities in-house, or can contract with the private sector for such capabilities*" (Swire and Ahmad 2012, 470) gaining access to the contents of communications

[26] As seen in recent requests by the FBI to gain access to an iPhone (Farivar 2016)

[27] More examples from this lens's point of view can be found in the quick-scan of government positions as part of the description of the current debate in chapter IV.

becomes problematic with encryption. A counter argument here is that old fashioned policework is still an option but there are factors that make this a lesser option: cost. No research is needed to conclude that a team tracking down and following a suspect to eavesdrop on conversations will be more costly than the ability to remotely listen in on phone conversations. We have not seen cost mentioned much but since all governments strive to become more efficient we assume it is also a factor.

From the point of view of one tasked with protecting a nation and its inhabitants from harm privacy matters a lot, as the loss of personal data can be particularly harmful, especially since phishing and ransomware attacks primarily target those services (often banking) that make use of encryption. In the interviews conducted as a part of the research into the coming into existence of the Dutch Cabinet position on encryption there was mention of the balance between privacy and security, more precisely: what amount of privacy are we willing to forsake for the sake of security?

The effects of backdoors

Looking at the effects of backdoors through a national security lens we can recognise that there are risks to a system of keys to backdoors but viewers using this lens will find that government agencies have a multitude of privacy infringing possibilities that they have handled responsibly for a long time.

The design of crypto systems that allow access by government agencies while not breaking the overall security of a system is continuously debated. A presentation by Apple at the 2016 BlackHat conference[28] has sparked particular debate. In the presentation Apple talked about the security of its mobile operating system (Krstic 2016). It led to one security blogger going as far as to tweet "*Still crazy how Apple went to BlackHat, told 1000 attendees how they build a secure crypto backdoor for their data center and nobody noticed*" (Tait 2016). While whether this is indeed what Apple showed is under much debate(Specter 2016)(Steve Bellovin 2016)(Green 2016), if one views the Going Dark problem from a national security lens this seems to open possibilities to securely deploy a backdoor in encryption. This would allow access to encrypted information without effect to privacy of those not part of the investigation.

Bringing it all together: the national security lens

Overall, a viewer applying this lens, while having a sense of risks for encryption as a whole and privacy in specific, concludes that the benefits outweigh the risks. The Golden Age of Surveillance may bring investigative agencies a tremendous amount of data but if the actual contents of communications cannot be exposed due to encryption there is little information to be gained.

III. The privacy lens

From a privacy or personal (as opposed to National) security point of view, encryption is more or less taken for granted as a key component of the Internet. When the Dutch Scientific Council for Government Policy reported on the public core of the Internet as a global public good, but pointed to a necessity of a new strategy to limit government interference with this public good, one of the ingredients mentioned was "*In order to protect the internet as a global public good there is a need to establish and disseminate an international standard stipulating that the internet's public backbone – its main protocols and infrastructure, which are a global public good – must be safeguarded against intervention by governments*" (Broeders 2015, 8).

Though we may naturally be inclined to trust our nation's investigative agencies to take great care of any keys to backdoors and only use these to their aid in investigations where terrorism or grave

[28] A global conference event series, in its 18th year in 2016, at which many security problems and solutions are presented and discussed by experts from all over the field.

crimes are concerned, this is far from certain. Next to the risks of a backdoor key being lost or leaked[29] there is the slippery slope of the causes the key is used for. The debate now focuses on terrorism but snooping into civilian communications can also be very useful in the investigation of lesser crimes. In addition to this risk an encrypted method that has a backdoor will see criminal (including terrorist) efforts shift either to making encryption for themselves or see them move towards not targeting hacking attempts at specific persons but towards find this 'golden' backdoor key, as that will allow them access to all communications done with the same encryption method. The analogy with the TSA locks for travel luggage we mentioned earlier comes to mind.

From a privacy point of view the access of government agencies to encrypted communications is taking the trade-off too far. Where those speaking from a government's point of view often refer to criminals and terrorists as a reason for wanting a backdoor, viewing the world through a privacy lens turns attention to the security and privacy necessary for banking, e-commerce, and everyday communication. Special attention is given to protection of freedom of the press, minorities or those with differing opinions living in authoritarian regimes. Last but not least the very governments that strive for special access could well fall victim to their own backdoors if keys to these doors fall into the wrong hands.

Protection of one's own life and liberties is an important notion here. Some take this even farther, noting that breaking of laws is sometimes necessary to move society forward. This point has some merit as in the past women had no suffrage, separation between people of different racial or cultural backgrounds was an everyday thing and people could go to jail for homosexuality. Citing examples like gay rights, and marihuana: "*How could people have decided that marijuana should be legal, if nobody had ever used it? How could states decide that same-sex marriage should be permitted?*" (Greenberg 2016a). The point being that without the possibilities of secret communication getting change underway is fruitless when a government is omniscient. In this case this conviction led Moxie Marlinspike to the creation of the Signal communications protocol, an end to end encryption method for phone messaging that is also the basis of WhatsApp's encryption.

Leaving examples like these aside the privacy lens views the debate from two basic premises:

Backdoors in encryption essentially break encryption from the inside out. (Further explained in the section on effects of backdoors in encryption).

And:

Backdoors in encryption are unnecessary for intelligence and detective agencies to do their work. (Further explained in the next section).

Effects of encryption

When viewed through this lens encryption is not seen to disadvantage investigative agencies to an extent that warrants backdoors, or other means of special access. And this is not merely an opinion of privacy advocates: former CIA and NSA Director Michael Hayden has said the country's (the US, in this case) intelligence agencies have methods to overcome the limitations presented by encryption, stating bulk data and metadata collection provides enough opportunity for investigation.(Howell O'Neill 2016a) Though he also named this mostly an issue for law enforcement as "*frankly, intelligence gets to break all sorts of rules, to cheat, to use other paths*" (Howell O'Neill 2016a).

[29] Not literally, but the digital nature of encryption would likely mean the access methods for governments can be copied and used by other parties if they gain access to systems used for backdoor access.

Another method that, though also debated[30], allows intelligence and law enforcement agencies to specifically target suspects without endangering the security of the Internet at large is Lawful Hacking. Described in a paper (Steven Bellovin et al. 2014) as the vulnerability option, concluding "*The use of vulnerabilities to accomplish legally authorized wiretapping creates uncomfortable issues. Yet we believe the technique is preferable for conducting wiretaps against targets when enabling other methods of wiretapping, such as by deliberately building vulnerabilities into the network or device, would result in less security*" (Steven Bellovin et al. 2014, 69).

Effects of backdoors in encryption

The relevance of the encryption debate is one for the Internet, and thus the world, as a whole. From a privacy point of view backdoored encryption equals no encryption. Which in turn means one of the fundamental pillars of cyber security is undermined by a threat of lawful access.

The parallel between the 90's debate and the current debate is clear. To further illustrate this, a group of scientists and experts that critiqued the Clipper era government proposal, stated:

"The deployment of key-recovery-based encryption infrastructures to meet law enforcement's stated specifications will result in substantial sacrifices in security and greatly increased costs to the end-user" (S. M. Bellovin et al. 1998, 9).

Surely, this is a statement that is equally applicable to the current debate. To add to this, a more recent paper (written by many members of the same aforementioned group) states as one of its key findings:

"We have found that the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago" (Abelson et al. 2015, 2).

Even if we take up the position of trusting our own government with a backdoor into our encrypted communications that does not mean we trust all governments. Yet all governments will want a backdoor from the same companies. This would necessitate a company to devise a cryptographic system with hundreds of additional keys (one for every agency with access per country that has regulations for this access) on top of the single pair of private and public keys per user that they would normally design.

We have already seen effects on cyber security due to backdoors in software, making clear that any action to add backdoor access to encryption will not only be beneficent to law enforcement and intelligence agencies but can also lash back to citizens, governments and commercial parties in a maleficent way. Many parties needed to switch over to different forms of cryptography when manipulation by the NSA on random number generators forming the basis of RSA security protocols become known (Menn 2014) and a team of researchers published a paper that indeed concluded exploitation possibilities were enhanced by it (Checkoway et al. 2014). More recently tools used by the NSA for their operations were stolen and were put up for auction (Weaver 2016).

The sentiment that backdoors are problematic is not merely a privilege for privacy advocates as, in a joint statement with ENISA, Europol stated on mandatory backdoors that "*While this would give investigators lawful access in the event of serious crimes or terrorist threats, it would also increase*

[30] Also in the Netherlands, as 'Hacking Back' by law enforcement is part of a new Dutch law proposal on computer crimes.

the attack surface for malicious abuse, which, consequently, would have much wider implications for society" (Europol and ENISA 2016).

Bringing it all together: the privacy lens.

From a strict privacy point of view a rational actor is expected to come to the conclusion that backdoors in encryption are essentially a bad idea. Those applying this lens to the debate will state backdoors will limit individual freedoms to a great extent whilst otherwise being futile in its attempt to limit the possibilities of those with bad intentions.

This lens seems to be gaining traction within the current episode of the 'Crypto Wars'. Perhaps this is unsurprising from a holistic point of view: when one takes everything in consideration even players that are mainly active in a national security context recognise that encryption is fundamental to many things and therefore neither the problem nor the solution.

IV. Reflections on this model

The three lenses described in the previous section provide three separate viewpoints on the same subject: encryption, encryption backdoors and their advantages and disadvantages. Though the angles are different actors employing either lens do so from rational arguments that lie within the framework their lens supplies them with.

In a way this goes back to long existing debates on the neutrality of technology. While it is often claimed that technology can never be neutral as not everyone has access to technology we feel it can be argued here that encryption is neutral for all users of the Internet. There may be a gap between those being able to get on the Internet and those who cannot but once Internet access has been achieved the encryption methods on it are freely available to and for all. Though there is an inherent value present in making the contents of one's communications secret the technical artefact used for this (encryption) is not inherently good or evil. Encryption is a central technology that underlies many things on the Internet, not just those on the 'Good' or 'Bad' side of things.

But perhaps this merely reflects our own academic viewpoint, purely reflecting Allison's rational actor lens in our expectation that players in this debate act as chess players "*moving the pieces with reference to plans and maneuvers [sic] toward the goal of winning the game*" (Allison 1969, 691). Though we are here perhaps viewing a game that cannot be won, where the only winning move is not to play[31] and leave things alone.

In many of the opinions ventilated through the media the essence seems to be that people tend to clash without trying to understand where the other party is coming from. A solution, or compromise is not achievable in terms of an exact position in a trade-off. What seems necessary is for actors to understand the differing viewpoint, accepting that differing viewpoints are possible, before starting on the road towards a viewpoint towards encryption that can be agreed upon. If we compare the viewpoints from our lenses this will be achievable by those utilising an economic or privacy lens, since they share the same conclusion. Compromise between this joint faction and those administering a lens of national security will prove harder.

To further aid understanding it must be noted that there is no difference between beneficiary and malevolent encryption, encryption is merely a tool that can be deployed by all, leading to a web of

[31] An option popularised as an opinion on nuclear warfare by the 1983 movie War Games, culminating in a scene where an Artificial Intelligence learns this from a game of Tic Tac Toe.
https://www.youtube.com/watch?v=NHWjlCaIrQo

interdependency, as illustrated in the figure below: encryption as a technology knows no right or wrong but rather finds itself in the middle of a vast field of actors each employing its possibilities to their own benefit.

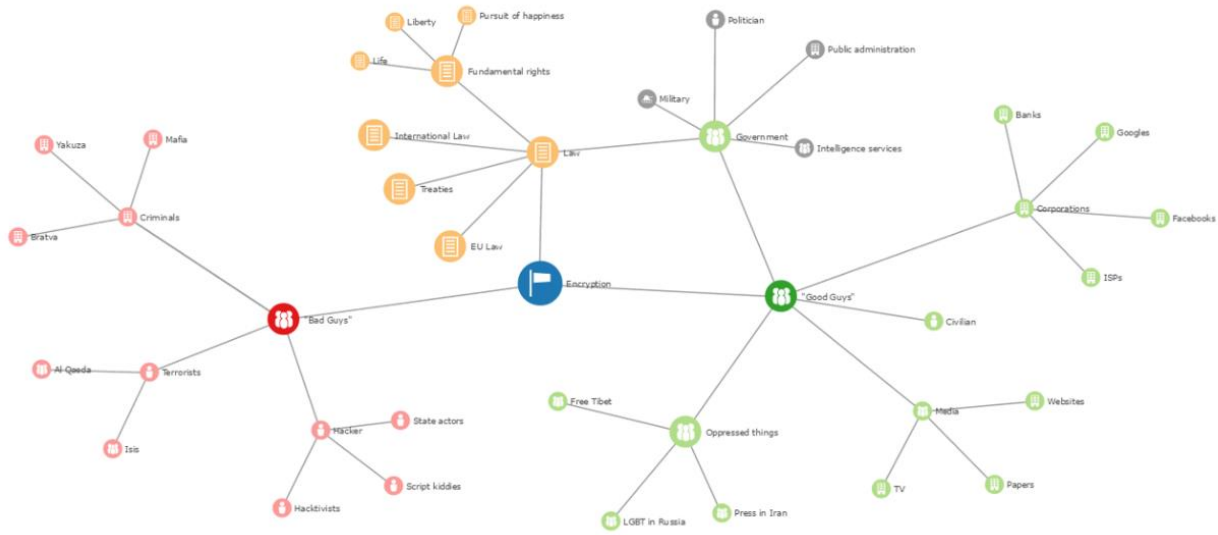

Figure 4: encryption web of dependency

To what extent different viewpoints, or the notion of interdependency on the same technology, are recognised by different actors is a subject for our next chapter, where we start our case study of the Dutch Cabinet position on encryption.

VI. The Netherlands and its official position

As we identified in our paragraph on the current debate, the Netherlands are currently the only country with an officially published Cabinet position on encryption. In summary, this position states the Dutch Government does not endorse any type of government mandated weakening of encryption algorithms.

On closer inspection, we see reflected in it the same three lenses we defined in our analytical chapter. An economic lens reflected in a section on "*The importance of encryption for the government, companies and citizens*" (G. A. van der Steur and Kamp 2016, 2) that states (amongst other things) that "*Confidence in secure communication and data storage is essential for the (future) growth potential of the Dutch economy, which is mainly in the digital economy*" (Ibid.). A national security lens reflected in a section on "*Encryption and the investigation, intelligence and security services*" (Ibid.) that recognises that encryption "*… complicates, delays or renders it impossible to (timely) gain insight into the communication for the benefit of protecting national security and investigating criminal offences."* (Ibid., 3). A privacy oriented lens reflected in a section on "*The right to respect for personal privacy and privacy of correspondence of citizens*" (Ibid) which includes the statement that "*… lawful access to information and communication by the investigation, intelligence and security services however[,] infringes on the confidential communication of citizens*" (Ibid.).

From the point of view of our lenses the Dutch position is balanced between the different views on encryption (economic, national security, privacy), leading to a rational result (the Dutch position) that combines all viewpoints, considering: "*There are currently no options in a general sense, e.g. via standards, to weaken encryption products without compromising the security of digital systems that*

use encryption. For instance, introducing technical access into an encryption product would make it possible for investigation services to inspect encrypted files, digital systems can become vulnerable to, for instance, criminals, terrorists and foreign intelligence services. This would have undesirable consequences for the security of communicated and stored information and the integrity of IT systems, which are increasingly important for the functioning of society" (G. A. van der Steur and Kamp 2016, 4) before ultimately concluding "*The cabinet is therefore of the opinion that at this point in time it is not desirable to take restrictive legal measures as regards the development, availability and use of encryption in the Netherlands*" (Ibid.).

Why the Netherlands came to such a position is the main subject of this chapter, and the main focus of this thesis. With the results of our interviews we will later answer our research question '*What process and factors within the Netherlands contributed to the forming of the Dutch official position on encryption?*'

As was described in our research method various interviews with actors who were either at the table during the process, in close contact with those at the table or involved indirectly, have taken place. This chapter presents the results of these interviews in a section called 'Process and formation of Cabinet position', which include a brief analysis of each interview in terms of our model from chapter V, and analyses the results in a section called 'Results of the process'.

I. Process and formation of Cabinet position

To gain more insight into the process that ultimately led to the Dutch Cabinet position we have performed several interviews. The following paragraph gives reports, per party interviewed, which each contain two sections: a report of the conversation and a reflection on where this actor is positioned from the point of view of our lenses.

Note that in all cases the report on the conversation is a paraphrased overview that should not be seen as official statements from the organisation involved. The information presented is a mix of official policy, personal observations and our analysis. Our goal was to shed light on the process that led to the Dutch position, not report on official policy of any of the parties interviewed.

Bits of Freedom

Bits of Freedom (BoF) is a digital rights organisation in the Netherlands, they are also part of the European Digital Rights (EDRi) association. This sets BoF apart from the Dutch Government but they were included in our interviews for several reasons: they supply Dutch organisations, including the government, with solicited and unsolicited advice on digital rights subjects, they wrote a position paper specifically on the subject of encryption and they are well-known in the Netherlands for hosting the annual Dutch Big-Brother awards (presented to individuals or organisations who took the year's most severe privacy threatening actions).

It will come as no surprise that BoF opposes any proposal that weakens encryption, posing the following in their short position paper on the subject "*The availability and use of high-grade encryption is essential for the protection of our digital infrastructure and communications. It is not only important for our democratic freedoms, but also vital for innovation and economic growth*" (BoF 2016, 2).

When asked in what way BoF contributed to the Dutch process they expressed that they indeed spoke to members of Dutch ministries and government but found it hard to point out what their actual influence on a process, as such that led to the Dutch Cabinet position, had been. From our information from the ministries and member of parliament we conclude BoF's influence was

substantial, with the representative for the Ministry of Economic Affairs stating they explicitly consulted BoF, as they are respected as knowledgeable on subjects that touch upon digital rights.

The aforementioned position paper by BoF was not directly mentioned by members of the government, perhaps unsurprising as the EDRi/BoF paper is dated the 25th of January 2016 whilst the letter to the Dutch second chamber containing the Cabinet position is dated the 4th of January 2016.

When asked what BoF sees as success factors to come to a widely supported government position on such a subject they mention: a realisation by policy makers that fundamental rights, the economy and the democratic state all gain from good encryption (realisation of this gain, according to BoF, seems to be increasing); Wide consensus outside of the government that backdoors are a bad idea, telecommunications companies, suppliers of ICT hard and software, and digital rights movements agree on this. BoF illustrated this by specifically noting that even Ronald Prins (CTO and CO-founder of Fox-IT, who are purveyor of encryption technology to the Dutch Government) sees backdoors as a bad idea.

BoF commented on the contents of the Dutch position that, though it is in essence a good statement (perhaps with the exception of the 'for now' addition towards the end of the statement), it would be more logical for the government to be more active and supportive of digital security by structurally investing in its development. The proposal from the Dutch Parliament to donate half a million euros to OpenSSL[32] development is seen as a nice gesture but as a small one that is not structural.

Analysis

BoF approaches the debate, non-surprisingly, from a privacy and personal liberties point of view. Their argumentation and conclusions reflect a rational approach that reveals little to none of any of Allison's other models, BoF is a small organisation[33] where organisational processes or political bargaining are less likely to result in different viewpoints.

Ministry of Defence

The Ministry of Defence, tasked with Dutch peace and security both within and outside the Netherlands, contains the Dutch military forces (Army, including the Dutch Cyber Command, Air Force and Navy), the Marechaussee (Military Constabulary and Border Police) and the Dutch Military Intelligence and Security service.

Representatives of this ministry were part of the sessions that led to the Dutch position on encryption. When asked about the origination and process of such a session we learned that the ministry tasked with the original questions takes the lead, checking who (which ministry) wants to adopt which parts that need to be worked out for a response, which was in this case in the form of a letter to the Dutch Parliament from the Dutch Cabinet.

The Ministry of Defence did not have an internal prior statement on the subject, though naturally opinions existed. The state of the Dutch law on the subject of encryption is ultimately the official position for the Ministry of Defence. The balancing act between security and privacy is in the domain of the legislator, not the ministries. The ministry seemly following a two-stepped approach, first to see 'what do we need to prevent things we do not want to happen' and then checking 'what may we do to try and prevent these'. This basis on legal foundations means the Cabinet position has not changed anything in the way of working for the Ministry of Defence as no laws were changed as a

[32] An open and free suite of cryptographic tools that is widely used on the Internet. For more information see https://www.openssl.org/.

[33] Their 2015 annual report states a total budget of about €500.000 and a workforce of 6.5 FTE (BoF 2015).

result of the position. This means that in essence the Netherlands does not undertake actions to generically weaken encryption. This was already the case and it remains so.

In our conversation, the ministry representative mentioned that the main actor within the department of Defence affected by the subject of encryption is the Military Intelligence Agency. Noting that they are caught in a split between security and privacy, which is also the case in the physical world as much as in cyber space. In an ideal world, everything is protected by strong encryption and the only privacy related impact due to investigations is faced by terrorists. The Ministry of Defence strives towards this ideal but realises its impossibilities.

The notion from a representative of the Ministry of Defence that security and privacy are seen as two values that largely correspond may seem positively enlightened to privacy advocates, when compared with ideas expressed by governments such as those in Hungary, the UK and Russia.

From a technological point of view ministry representatives who have to work with encryption in practice were involved in the sessions.

When asked about success factors that contribute to achieving consensus within a Cabinet on a subject like encryption 'parliamentary control' was mentioned as the basis of coming to legitimate statements. A key notion mentioned was that the Cabinet position on encryption probably would not have arisen without parliamentary questions. Remarks from digital rights movements may influence public debate and thus members of parliament but the Cabinet only has a responsibility to answer questions from parliament, making those questions a more likely trigger for changes in policy . Awareness, though a bit of a clincher, remains an important point, the distance between technical experts and policymakers remains large. Blending of people with different backgrounds also seems to have helped the process along.

When economic angles were discussed the value of working with partners in the private sector was mentioned. Dutch Telco KPN is an important partner for the Ministry of Defence for communications needs, there is no benefit for ministries, or the government, to put forward a position that is harmful for partners (like KPN) they depend upon.

In the process of the interview cost was briefly mentioned as a minor factor for the move of intelligence operations into the digital field. These operations are often more cost efficient due to less personnel being necessary for digital investigations as opposed to investigations in the physical world.

Analysis

A ministry with many different departments will naturally exhibit a more complex set of behaviour than a civil liberties organisation like Bits of Freedom. As the Ministry of Defence contains both parts that are dependent on encryption for their own secure communications and parts that are thwarted by encryption in their strife towards a better view on possible threats to the Netherlands, it is highly likely that the input from the Ministry of Defence is a result of organisational process factors and possibly political bargaining with other departments. However, we cannot conclude about this based on our single interview. What we can conclude is that the Ministry of Defence, despite having a responsibility in national security, presents a view on the encryption debate that, from a rational actor point of view, reflects more than just the national security lens, as security and privacy are seen as values that interlock.

Ministry of Security and Justice & National Cyber Security Centre

The Dutch Ministry of Security and Justice has responsibilities ranging from the public prosecution service to security (including cyber security through the National Cyber Security Centre) and counterterrorism. This inherently presents this ministry with tasks that may seem irreconcilable: keeping the Netherlands and its citizens secure both online and offline, both against terrorists and against (foreign) government intrusion.

The Dutch Cabinet position on encryption was primarily signed by Ministers van der Steur (Security and Justice) and Kamp (Economic Affairs), how this came to be was one of the first items to be discussed. As was mentioned before the whole affair gained traction due to questions from the Dutch Parliament (from D66's Kees Verhoeven), which were picked up by Minister Kamp, together with his colleague from the Ministry of Security and Justice, van der Steur. Civil servants from the Ministries of Economic Affairs and Security and Justice immediately broadened the scope towards multiple ministries, recognising that this was not a mere economic or security and justice issue. Exact details of dates did not come to mind during our meeting but the general recollection was that the process started somewhere in May or June of 2015.

The point mentioned in our interview with the Ministry of Defence, that a Cabinet position would not have appeared without questions from parliament, was seen as likely. The subject was important within the Ministry of Security and Justice but the end result might have been used solely for the benefit of internal understanding if the subject hadn't been brought to generic Cabinet attention.

When speaking of the success factors that led to the consensus necessary to come to a joined Cabinet position, a number of things were mentioned: the way in which policy options and needs from different departments were examined and worded in the Cabinet position is seen as of particular interest; The position does not jump to a conclusion but carefully deliberates on what different interests are (civil rights and security for citizens and companies alike, lawful access and investigative options for investigation and security services) before ultimately concluding limitations to encryption are disadvantageous for all.

The National Cyber Security Centre (NCSC), was involved for expertise from the technical side, answering our question if any technical or technological factors were part of the discussions. The NCSC was involved to keep information and ideas factual about the technological side.

Following the publication of the Cabinet position there have been some additional questions from parliament, particularly concerning the AIVD Chief Bertholee's interview in the Dutch Volkskrant (Modderkolk 2016) and the Dutch Public Prosecution Service also expressed a wish to gain access to encrypted information (Schellevis 2016) (though the prosecutor who expressed this later tweeted they did not want to weaken encryption (Egberts 2016)). This later set of publications concerning the Cabinet position was discussed during the meeting, noting that these, alongside the position itself, form an important set of documentation for the Dutch policy surrounding the subject.

When asked about information from the aforementioned Bits of Freedom the existence of knowledge of positions of such organisations was affirmed. Though the influence is indirect: as a part of policy creation many parties, within and outside of the government, are consulted to gain a generic overview of ideas throughout society.

Though the Cabinet position has not changed any laws or ways of working within government departments, having a statement in print is seen as a new basis in both national and international discussions: the position of the Netherlands can be made clear simply by means of the Cabinet's statement.

Analysis

Both the Cabinet position and the information expressed in this interview mention a three-angled view at encryption which is also reflected in our lenses: economic/society, investigative/intelligence (national security) and privacy. Perhaps this added to the Dutch end result due to the influence of a balanced view (a representation of Allison's model I) on organisational process (Allison's model II).

Ministry of Economic Affairs

The Netherlands has a combined Ministry of Economic Affairs, Agriculture and Innovation. From an encryption point of view impact on agriculture may be less of a concern but innovation and economic affairs have a stronger dependency. The Authority for Consumers and Markets (ACM), while independent, is also part of the Ministry of Economic Affairs, from a juridical point of view.

For this ministry, the impact of changes to encryption law is seen in terms of effects to citizens and companies as parts of the economy. The Minister for Economic Affairs, Henk Kamp, was addressed in the questions from parliament, resulting in this ministry starting up the formation of an answer. The Ministry of Security and Justice was named as a logical partner as they have a wide responsibility in all things cyber. For the ensuing process representatives from other ministries were included to ensure an adequate span of government interests. For the Ministry of Economic Affairs unencumbered relations with market actors (who should have unimpeded access to encryption technologies), the guarding of trust in the Internet, and transparency about government policy are important factors.

The process of writing a joint Cabinet statement was described as starting off with a clear division and mix of opinions surrounding the subject, changing into a mode where everyone's particular interests were articulated and only then exploring if there was a way to accommodate all these interests at the same time.

An interesting piece of input was formed by a document prepared for the Obama administration in the US, in which options for backdoors are explored but the end conclusion is that all options have drawbacks (Anonymous 2015)(Peterson and Nakashima 2015)[34]. This conclusion added to a realisation that there is no satisfactory way to solve the issue.

Though it is recognised that investigative agencies need tools to fulfil their tasks, proportionality is mentioned as important. The result is that encryption is seen as something that cannot be weakened, only broken. This is regarded as non-proportional and thus undesirable.

Before talks about the Cabinet position commenced various parties were asked for input, including BoF, who were mentioned as a supplier of objective sources that answered questions at hand. Other external factors are estimated to be fairly minimal for this Cabinet position. Though, both from a Defence and Economic Affairs point of view, market players were considered. The Ministry of Defence is dependent on market players for their communications and government regulations about communications have an economic effect on the same players.

When asked about contacts with other countries information was limited, though the Dutch position has been translated into English and was mentioned to be widely distributed amongst EU member states.

From a strictly economic viewpoint most current growth is achieved through the application of ICT in the various sectors of the Dutch economy, which is influenced by government regulations on ICT.

[34] We found the anonymous report via the Washington post news article, whether this is the same way it reached the Dutch Government is unknown.

One thing mentioned was the settling of companies in the Netherlands has dependencies with a clear position on encryption. Though apparently, market players in the Netherlands (apart from the telecommunications sector) have not asked the Ministry of Economic Affairs questions on the subject. The encryption dossier started rather quietly in April of 2015 for this ministry, but the Cabinet position and international discussions about things like encryption in WhatsApp have put it on the agenda.

From the Ministry of Economic Affairs' perspective, the Cabinet position has changed things, resulting for instance in the Dutch Government now donating funds for development of strong (open) encryption standards (Miltenburg 2015), which is also due to a motion by Dutch Parliament Member Kees Verhoeven on the subject.

The 'for now' addition to the Cabinet position, that can possibly be seen as an opening for those government parts wanting more access to encrypted data, is seen as somewhat confusing but ultimately minor as policy, whatever it states, is by definition temporary. Policy can always be changed due to developing circumstances.

The name of D66 parliamentarian Kees Verhoeven was mentioned again, as someone who constantly keeps this issue on the agenda.

Success factors from the Ministry of Economic Affair's point of view was this starting point of considering the interests and problems of separate departments before trying to come up with a solution. The presence of a cryptographic expert from the NCSC[35] is seen as important, both due to expertise in subject matter and an impartial role in the process. Dutch consensus culture, though not directly mentioned, is present in the mention of participants who are able to allow others to describe their challenges without continuous discussion.

Analysis

Though expressing the benefits of a wide and understanding approach to viewpoints from other ministries, the representative for the Ministry of Economic Affairs we spoke to stresses the economic impact of government induced weaknesses in encryption. As the start of developments towards a Cabinet position was again tied to the questions that came from parliament, little organisational process influencing the debate from within this ministry seems present. Argumentation from the Ministry of Economic Affairs closely resembles the points we made in our superimposition of the economic lens over Allison's model I.

Members of Parliament

As is the case in other countries that form a parliamentary democracy, the second chamber of Dutch Parliament has a role in monitoring the Dutch Cabinet's actions. As was mentioned in the reports of other interviews the forming of the Cabinet position started after questions from parliament. While the Internet and ICT portfolio is present at the majority of Dutch parties few of them seem to specialise in the subject, one notable exception being the D66 party who went as far as presenting a "Techvisie" (Verhoeven et al. 2016), in which they present their view on the future of technology and the Internet in relation to society. This vision includes a section on "Encryptie als grondrecht" (Verhoeven et al. 2016, 60), which literally translates into "Encryption as fundamental right", which further describes the necessity of strong encryption from the angle of both democratic liberty and the economy.

[35] Who we interviewed as representative from the NCSC.

The D66 party is not the only active participant in parliamentary debates about encryption, members of the PVDA and SP parties also take part in these debates but from what we have seen Kees Verhoeven of D66 is the most active (which is also reflected in other interviews we conducted). The information in this paragraph is from our interview with the D66 contributor for ICT, who is also one of the authors of the aforementioned “Techvisie”.

The process that led to the Cabinet position is a bit of a black box from the point of view of parliament. Questions are asked and ministers state they will reply at a certain date but from this point on it is mainly a waiting game, those asking the questions are not consulted in the meantime.

The starting point of this debate from the parliamentary point of view seems to lay around May of 2015, when questions were asked in debates about topics for the Ministries of Security and Justice, and Economic Affairs, which also resulted in a motion to supply funds to open source encryption initiatives.

For D66 strong encryption is seen as an item that keeps gaining in importance, reflected not only in questions to the responsible ministers but also in the presentation of their technological vision and the regular challenges and renewed questions to the Cabinet about the position on encryption.

Looking deeper into this vision document, especially the acknowledgements, many persons are mentioned, including several people from Bits of Freedom, including Rejo Zenger (again showing at least that their contributions to various debates are heard).

The statement that ‘A Cabinet position would likely not have emerged had parliament not asked questions’ was again seen as likely. Technical knowledge is noted to be more important than for other subjects, which D66 sees in proposals and explanations that arise from parties who do not employ experts in the subject matter, awareness on this issue is apparently still limited.

When asked about success factors to come to a widely-supported view of a subject like encryption, the parliamentary angle supplied a new perspective on things: the effects of a multi-party system. In contrast to countries like the UK or the US, which traditionally have two large parties and a limited set of smaller ones, the Netherlands has a vast array (currently around 15) of political parties, none of whom usually have a chance to become a majority on their own. A result of this is that parties may look for niche’s in policy that other parties have not addressed, or not strongly addressed. In this case this meant D66 saw (Internet) technology and the debates connected to it (including encryption) as a change to reach a portion of the electorate that was not addressed by other parties.

The nascence of the Cabinet position has brought along the continuous attention of Dutch Parliament members to debates where encryption is relevant, resulting in requests to reaffirm the statement and promoting it in the international context. The Netherlands is ahead of the rest of the world in several Internet related areas of policy (net neutrality, responsible disclosure and the position on encryption being the most relevant examples) which is seen as gathering influence in its own right.

The presence of the ‘for now’ limitation in the Cabinet position is, though not remarked as positive, seen as a minor point as positions can always be changed by future governments.

Analysis

In our conversation, the points discussed touched upon deliberations we mentioned in the economic and privacy lenses through which to view the encryption debate. Political parties, and their representatives in parliament, express thoughts and opinions based on their particular party programs. Though we cannot be sure how much organisational process factors are in play due to the

limitations of our research, our estimation based on the interviews conducted is that these will be less for a party like D66 than for any ministry.

II. Results of the process

To be sure, the main result is the "Kabinetsstandpunt Encryptie" (V. der Steur and Kamp 2016)[36] by the Dutch Government. The fact that a government came to an official position on this while the debate was still ongoing worldwide was news in itself but it was mainly picked up by a great variety of news sites (Moody 2016)(BBC 2016)(Hackett 2016)(Schneier 2016) due to the aforementioned conclusion of the position:

"The cabinet endorses the importance of strong encryption for internet security to support the protection of personal privacy of citizens, for confidential communication of the government and companies and for the Dutch economy.

The cabinet is therefore of the opinion that at this point in time it is not desirable to take restrictive legal measures as regards the development, availability and use of encryption in the Netherlands." (G. A. van der Steur and Kamp 2016, 4)

As to why developments towards a Cabinet position started in the first place our answer is clear: Questions from D66 parliamentarian Kees Verhoeven. This was mentioned by all those involved from the ministries we spoke to. A report which reached us later, of a general meeting of the council for transport, telecommunications and energy on the 15th of June 2015, seems to confirm this (Vermeij, Azmani, and Franke 2015). In it Verhoeven asks for Kamp's view on backdoors, to which Minister Kamp replies that he will look into it, possibly together with his colleague from the Ministry of Security and Justice, and will come back to it at a later date[37].

In the end the Cabinet position will have been a result of organisational process in the government and political bargaining between the actors involved. But, as we mentioned as one of our limitations, conclusions from Allison's model II and III are hard to support based on our limited set of interviews. When listening between the lines of our interviews, however, we dare say organisations like Bits of Freedom and Members of Parliament for a specific party will suffer the influences of organisation processes and governmental politics less than those working within a ministry.

An interesting point of note is the role of the Dutch digital rights organisation Bits of Freedom (BoF). Though they expressed having given advice to different governmental actors on various occasions, BoF was hesitant to comment on their influence. From our interviews with representatives of both ministries and parliament we conclude their voice is heard, respected and was taken into consideration in the process that finally resulted in the Dutch Cabinet position.

As to the consequences of this official position for governmental operations the results were mixed. In the viewpoint of the Department of Defence little has changed as there was no change to laws that govern the way intelligence can be done. Governmental colleagues from the Justice Department and Economic Affairs, while recognising that no new laws were created, do note that the position eases discussion on the subject as the statement is very clear. For parliament members dealing with an ICT portfolio the Cabinet position seems an anchor they keep referring to in bringing Dutch cyber policies forwards.

[36] This is the original Dutch version. For reasons of clarity all quotes and referrals are to the official version available in English.

[37] Translation and paraphrasing by the author. Original remarks (in Dutch) can be found on page 11 of the document referred.

After publication of the Cabinet's view two interesting cases followed in 2016: the interview the Dutch news agency NOS had with a Public Prosecutor that mentioned a lack of access to encrypted data being problematic and the interview Dutch newspaper the Volkskrant had with the head of the Dutch Intelligence Service, who also voiced such sentiments. Both were followed up by questions to the Cabinet from parliament and the last of these debates ended with the Cabinet's reaffirmation of the existing position in October of 2016 (van Voorst 2016).

How the information from our interviews helps us answer our research question is the subject of the next chapter.

VII. Findings

The extent to which our research questions can be answered vary. For our first question: '*How can we understand the decision-making of political actors in the Dutch public sector within the encryption debate?'* we can attest that starting from the point of view of Allison's models and combining these with our superimposed economic, national security, and privacy lenses, has allowed for a broad analysis of the encryption debate in general. Through this we can understand why, though based on differing arguments, those from an economic and privacy background can be expected to agree that putting any form of backdoor in encryption is essentially a bad idea. While at the same time the lenses also help us understand why rational actors responsible for national security search for a lawful way to trade the privacy of some for the security of others. The answer of our research question cannot be stated in these few simple sentences but is rather represented by our chapter V about viewpoints on encryption.

Developing a model such as Allison's, with the addition of our lenses, helps clarify why differing viewpoints exist, and what merits they have. Applying this model to generic information available about countries is possible but involves a lot of guesswork. Applying such a model to interviews with a specific actor from (in our case) ministries is harder and end up heavily in Allison's rational actor corner, organisational process ideas are hard to discern when information from a single actor is analysed and the same is the case when trying to decide whether something is a rational choice or a result of political bargaining.

For our second research question '*What process and factors within the Netherlands contributed to the forming of the Dutch official position on encryption?'* we can distil a more condensed outcome, primarily from our interviews. From a process point of view the initiation is found in the basic democratic principle through which parliament asks responses from the government. The way this was followed through by the responsible ministers reflects Dutch consensus culture (the 'Poldermodel'), resulting in a Cabinet wide debate, and statement, on the subject of encryption. Other factors that played a role are the Dutch political system where many small parties, in their efforts to reach the electorate seek out niches that were hitherto not addressed, encryption proved to be such a niche. Another factor is the presence of trusted technological expertise, in this case brought to the table by the Dutch NCSC, which allowed those with an economic, defence, or security and justice agenda to rely on an outsider (of the political process) to keep things sensible from a technological point of view. The presence of an active digital rights organisation (Bits of Freedom, in the Dutch case) also seems to be a factor, as their name, and that of the person we interviewed kept being mentioned.

We find the influence of information from other governments, like the research done by the Obama administration, harder to value. Likewise, the dependence of the economy in general to the ICT

sector makes transparency about a governments intention with encryption an important factor, but (though we have not researched this) ICT is a driving force behind economic growth in many countries, not just the Netherlands.

While our outcome to this question represents statements from the parties we spoke to they are generally not solely based on output from a single party. Some examples of this can be seen in the presence of NCSC expertise, which was mentioned as beneficial by multiple parties, as was the input from Bits of Freedom. And though the splintered nature of the Dutch Parliament leading to niches was only mentioned by our representative for parliament, we see the implication of this reflected in the fact that the resulting parliamentary questions were indeed picked up and addressed by the Cabinet.

Though we can identify factors that will be helpful in any country, answers to our third research question '*To what extent can success factors for the development of an official position be derived from the Dutch case?*' will be very preliminary. The Dutch situation has a couple of recognisable success factors that can be abstracted but are nonetheless hard to implement on a generic level: a political situation with a lot of smaller parties may create a climate for niche development of opinions that are debated in both parliament and Cabinets alike, but this does not seem a development that can be steered or is beneficiary per se. Correspondingly the presence of a digital rights organisation can only indirectly be promoted by a government but civilians feeling a need to influence government can join the organisations present in their respective countries (many countries already have such organisations, their influence on governments will vary). The consensus culture known as the Dutch 'Poldermodel' has been a matter of discussion for much longer than the encryption debate and may prove even harder to influence.

Factors that can be influenced by a government more directly also exist. Many countries have a National Cyber Security Centre, in the Dutch case the presence of an expert from their NCSC was beneficial to the process. In a way this reflects a notion the Dutch Scientific board stated "*It is therefore vital to advocate internationally for a clear differentiation between internet security (security of the internet infrastructure) and national security (security through the internet) and to disentangle the parties responsible for each*" (Broeders 2015, 9).

To conclude the answering of this question we feel that research into what we can abstract from this case study would need future work.

VIII. Conclusions & future work

Summary and contribution

The importance of the Internet in our communications is still increasing, for everybody on the planet, thus including criminals and terrorists. The wish to have some form of control over the communications done by criminals and terrorists by means of the Internet is understandable, but this can only be done at the expense of the privacy of communication by all other users of encryption (in essence: everyone else). What results is a clash of opinions where common ground is sought.

Perhaps ultimately there is no single solution, the different lenses that are employed whilst analysing current affairs inherently mean irreconcilable differences in opinion will remain present. But we hope that the realisation that different actors apply different lenses will allow for a debate with more mutual understanding.

This thesis has explained the debate surrounding encryption and the proposed circumvention of it by government agencies. We have described the historic context provided by earlier instances of this debate and supplied illustrations from a selection of countries to depict the current debate. Subsequently differing viewpoints on encryption were analysed based on their own merits and flaws. Using all insights and information thus collected we analysed the nascence of the Dutch Cabinet position via the means of interviews with those who were part of, or close to, the formation of the position by the Dutch Cabinet. The latter showing a distinct set of factors that culminated in the creation of the Cabinet position, though abstracting these to a level in which they are usable by other countries may prove difficult.

As to our contribution to the field of academic research into (cyber security) governance relating to the subject of encryption, we have supplied insights into the emergence of the Dutch position on encryption, identified the dominant angles of relevance in the encryption debate (economy, national security, privacy), and bundled a great number of sources on the subject during the effort.

Future work

During our research we identified several subjects that seem open for further research.

Encryption governance overview. We have only performed a quick-scan of debates in countries, selecting those that aided in the description of the current debate. A complete overview of countries, what their position on encryption is and perhaps plotting these on an economic/national security/privacy scale is sure to provide insights in global developments. This could also benefit, or add to, publications that already report on Internet freedom.

Generalisation of the Dutch case. Though we shared some preliminary thoughts on the abstracting of generic success factors from the Dutch case we did not pursue this avenue to any depth. Perhaps there is a sure way to come to a balanced government standpoint on this debate if certain economic or political conditions are met. The topic is an interesting one from a public administration point of view. Perhaps testable propositions can be defined and researched.

Relation between terrorism and encryption legislation. We have seen that countries that experienced terrorist attacks seem to deliver the strongest argumentation for more police and secret service access to (encrypted) data. It would be interesting to research if this is indeed a relation that spans further than France, the UK and the US. It may seem obvious that there is a positive relation (more terrorist attacks lead to more wishes for lawful access) but common-sense assumptions have been proven wrong before.

Strong backdoored encryption. From a government point of view, developments to cryptography that can provide strong encryption while at the same time allowing access to individual messages without creating the tools to read them all, are desirable. From a governance point of view it is easy to make such a demand but whether or not cryptography can ever solve this is beyond our understanding of the matter. We expect this will already be a research item for cryptographers.

Further study of the Dutch case. Diving deeper into what Allison's model II and III can teach us about the Dutch situation will demand more information from more actors present during the various sessions that culminated in the Dutch Cabinet position.

Conclusion

Our thesis has shown that, supplied with the proper frame of reference, opposing factions' positions in the encryption debate can be understood in their own right. Using this frame as a backdrop for the

interviews we conducted in our case study of the Dutch situation has shown the latter to be not a chance occurrence but rather the result of a number of distinguishable factors.

On the encryption debate as a whole we perhaps need to conclude that the end goals of being perfectly secure and being perfectly in control are mutually exclusive, so a form of middle ground will need to be found, though it will always be debated.

We will sign off with the sole hypothesis in this thesis: we will see another instalment of the 'Crypto Wars'. Perhaps when quantum-encryption becomes a common technology or when all interhuman communication moves from cyber space into virtual reality space. Whatever the trigger may be, government agencies shall once again feel a need to have special access to new ways of communicating. This will perhaps be due to technology inconceivable today but when next communication shifts to a new medium 'Crypto Wars' about rules and regulations are likely to follow.

Appendix 1: interview questions

Preface

Questions were not supplied to interviewees beforehand nor addressed in any particular order. At the start of interviews our research was briefly explained after which discourse more or less ran freely. The following is an overview of questions and topics we used as a reference to address our research questions.

Questions / Topics:

- How was your organisation part of the debates that led to an official Cabinet position?
- Why do you think the Netherlands was able to come to an official Cabinet position?
- How does your organisation think Dutch political processes differ from other nations?
- How does your organisation think different backgrounds (lenses) influenced different viewpoints?
    - Was this a known factor when devising the Cabinet position?
- How does your organisation view European/International developments?
    - i.e. the French/German opinion on this, US developments and UK viewpoints.
    - Were European (or other International) debates an influence?
- Was encryption a point of discussion before current affairs brought it to the forefront?
    - i.e. terrorist attacks or criminal cases where end to end encrypted communications were used
    - Did a position, or opinion exist before the debate became current?
- What were things that aided policy developments, and what were things that hindered?
    - What aided or limited discussion?
- Which departments were involved?
- Was analysis done from different viewpoints?
- Was there a background in political party programs?
    - Was this an issue in debates?
- Why do you think the Netherlands was able to get to a firm position on this subject?
- How is the Netherlands promoting its Cabinet position in the rest of the EU?
    - Especially in light of recent French/German opinions on this.
    - In light of Slovakian EU chairing and their wish to put encryption on the political agenda
- Do you have insights into why other countries have not come to an official position?

Appendix 2: interview details

Preface

Interviews were not recorded nor precisely transcribed but extensive notes were taken. Should questions arise about the interviews the thesis author can be contacted.

Overview of interviews.

Bits of Freedom
Rejo Zenger, blogger, advisor and technology expert. Interviewed on Tuesday October 18th 2016, by phone.

Ministry of Defence
Eelco Karthaus, Senior Policy Officer. Interviewed on Thursday October 20th 2016 in The Hague.

National Cyber Security Centre
Technical Expert. Interviewed on Tuesday November 1st 2016, in The Hague, alongside the Senior Policy Officer of the Ministry of Security and Justice.

Ministry of Security and Justice
Senior Policy Officer. Interviewed on Tuesday November 1st 2016, in The Hague, alongside the Technical Expert of the National Cyber Security Centre.

Ministry of Economic Affairs
Ronald van der Luit, Senior Policy Officer. Interviewed on Wednesday November 2nd 2016, in The Hague.

Dutch Parliament
Marijn van Vliet, contributor to Dutch Parliament member Kees Verhoeven (for the D66 party) on subjects of ICT. Interviewed on Friday November 25th 2016, in The Hague.

Bibliography

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, et al. 2015. "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications." *Journal of CyberSecurity* 0 (0): 11. doi:10.1093/cybsec/tyv009.

Agencia EFE. 2016. "Brazil Supreme Court Overturns Judge's Ruling Blocking WhatsApp." *Efe.com*. http://www.efe.com/efe/english/world/brazil-supreme-court-overturns-judge-s-ruling-blocking-whatsapp/50000262-2990118.

Allison, Graham T. 1969. "Conceptual Models and The Cuban Missile Crisis." *The American Political Science Review* 63 (3): 689–718.

Anderson, Luke. 2015. "Estonian Government: Leading The Way In Secure Digital Authentication." *Purehacking.com*. https://www.purehacking.com/blog/luke-anderson/estonian-government-leading-the-way-in-secure-digital-authentication.

Anderson, Ross. 1994. "A5 (Was: HACKING DIGITAL PHONES)." *Uk.telecom Newsgroup*. https://groups.google.com/forum/#!msg/uk.telecom/TkdCaytoeU4/Mroy719hdroJ.

Anonymous. 2015. "Read-the-Obama-Administrations-Draft-Paper-On.pdf." https://assets.documentcloud.org/documents/2430092/read-the-obama-administrations-draft-paper-on.pdf.

Arora, Mohit. 2012. "How Secure Is AES against Brute Force Attacks? | EE Times." *Eetimes.com*. http://www.eetimes.com/document.asp?doc_id=1279619.

Baker, Jennifer. 2016. "Encrypted Messaging Apps Need Backdoors, Says Top Dutch Spook." *Arstechnica.co.uk*. http://arstechnica.co.uk/tech-policy/2016/09/encrypted-messaging-apps-backdoors-dutch-secret-service-chief/.

Baker, Stewart A. 1994. "Don't Worry Be Happy." *Wired*. https://www.wired.com/1994/06/nsa-clipper/.

Ball, James. 2015. "Cameron Wants to Ban Encryption – He Can Say Goodbye to Digital Britain | James Ball | Opinion | The Guardian." *Theguardian.com*. http://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror.

BBC. 2015a. "Charlie Hebdo Attack: Three Days of Terror." *Bbc.com*. http://www.bbc.com/news/world-europe-30708237.

———. 2015b. "Paris Attacks: What Happened on the Night." *Bbc.com*. http://www.bbc.com/news/world-europe-34818994.

———. 2016. "Dutch Government Says No to 'Encryption Backdoors.'" *BBC.com*. http://www.bbc.com/news/technology-35251429.

Bellovin, Steve. 2016. "Does Apple's Cloud Key Vault Answer the Key Escrow Question?" *Columbia.edu*. https://www.cs.columbia.edu/~smb/blog/2016-08/2016-08-24.html.

Bellovin, Steven, Matt Blaze, Sandy Clark, and Susan Landau. 2014. "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet." *Northwestern Journal of …* 12 (1): 1–66. http://goodtimesweb.org/surveillance/2013/lawful-hacking.pdf.

Bellovin, Steven M, John Gilmore, Peter G Neumann, Ronald L Rivest, Jeffrey I Schiller, and Bruce Schneier. 1998. "The Risks of Key Recovery, Key Escrow & Trusted Third Party Encryption." *Digital Issues*, no. 3.

Bendor, Jonathan, and Thomas H. Hammond. 1992. "Rethinking Allison's Models." *The American Political Science Review* 86 (2): 301–22.

Bennett, Cory. 2016. "Senate Encryption Bill Draft Mandates 'Technical Assistance.'" *Thehill.com*. http://thehill.com/policy/cybersecurity/275567-senate-intel-encryption-bill-mandates-technical-assistance.

Berman, Mark. 2016. "UN Human Rights Chief Backs Apple in Encryption Fight." *Thestar.com*. https://www.thestar.com/business/2016/03/04/un-human-rights-chief-backs-apple-in-encryption-fight.html.

Bienkov, Adam. 2015. "David Cameron: Twitter and Facebook Privacy Is Unsustainable - Home Affairs." *Politics.co.uk*. http://www.politics.co.uk/news/2015/06/30/david-cameron-twitter-and-facebook-privacy-is-unsustainable.

Bird, Richard. 2016. "China's Rules on Encryption: What Foreign Companies Need to Know." *Freshfields.com*. Accessed December 21. http://www.freshfields.com/en/global/Digital/China_rules_on_encryption/.

Blaze, Matt. 1994. “Protocol Failure in the Escrowed Encryption Standard.” *Proceedings of Second ACM Conference on Computer and Communications Security*, no. April 1993: 59–67.

Blomfield, Adrian. 2007. “War of Words over Bronze Soldier.” *Telegraph.co.uk*. http://www.telegraph.co.uk/news/worldnews/1541641/War-of-words-over-bronze-soldier.html.

Bode, Karl. 2015. “After Endless Demonization Of Encryption, Police Find Paris Attackers Coordinated Via Unencrypted SMS.” *Techdirt.com*. https://www.techdirt.com/articles/20151118/08474732854/after-endless-demonization-encryption-police-find-paris-attackers-coordinated-via-unencrypted-sms.shtml.

BoF. 2015. “Jaarverslag 2015.” https://2015.bof.nl/bits-of-freedom-jaarverslag-2015.pdf.

———. 2016. “Position Paper on Encryption.”

Brabant, Malcom. 2015. “Copenhagen Shootings: Why Denmark Was Steeled for Terror Attack.” *BBC.com*. http://www.bbc.com/news/world-europe-31478148.

Braga, Matthew. 2016. “Why Canada Isn’t Having a Policy Debate over Encryption.” *Theglobeandmail.com*. http://www.theglobeandmail.com/technology/why-canada-isnt-having-a-rigorous-debate-over-encryption/article28859991/.

Broeders, Dennis. 2015. “The Public Core of the Internet: An International Agenda for Internet Governance.” *WRR-Policy Brief*, no. 2: 20.

Budington, Bill. 2016. “WhatsApp Rolls Out End-To-End Encryption to Its Over One Billion Users | Electronic Frontier Foundation.” *Eff.org*. https://www.eff.org/deeplinks/2016/04/whatsapp-rolls-out-end-end-encryption-its-1bn-users.

Buttarelli, Giovanni. 2016. “Preliminary EDPS Opinion on the Review of the ePrivacy Directive.”

Castro, Daniel, and Alan Mcquinn. 2016. “Unlocking Encryption : Information Security and the Rule of Law.” *Information Technology and Innovation Foundation*, no. March: 1–50.

Checkoway, Stephen, Matthew Fredrikson, Wisconsin Madison, and Ruben Niederhagen. 2014. “On the Practical Exploitability of Dual EC in TLS Implementations.” *USENIX Security 2014*, 319–35.

Comey, James B, and Sally Quillian Yates. 2015. “STATEMENT OF DEPUTY ATTORNEY GENERAL DEPARTMENT OF JUSTICE AND FEDERAL BUREAU OF INVESTIGATION BEFORE THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE ‘ GOING DARK : ENCRYPTION , TECHNOLOGY , AND THE BALANCE BETWEEN PUBLIC SAFETY AND PRIVACY ’ PRESENTE.”

Conger, Kate. 2016. “Burr-Feinstein Encryption Bill Is Officially Here in All Its Scary Glory.” *Techcrunch.com*. http://techcrunch.com/2016/04/13/burr-feinstein-encryption-bill-is-officially-here-in-all-its-scary-glory/?ncid=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%253A+Techcrunch+(TechCrunch)&utm_content=FaceBook&sr_share=facebook.

Corera, Gordon. 2015. “How NSA and GCHQ Spied on the Cold War World.” *BBC.co.uk*. http://www.bbc.com/news/uk-33676028.

Council of the EU. 2016. “Input Provided by MS on Questionnaire on Encryption in Criminal Cases.” *Asktheeu.org*. https://www.asktheeu.org/en/request/input_provided_by_ms_on_question?nocache=incoming-11727#incoming-11727.

Cushing, Tim. 2016. “Why Encryption Bans Won’t Work: Brazil Government’s WhatsApp Block Just Sends Users To Other Encrypted Platforms.” *Techdirt.com*. https://www.techdirt.com/articles/20160507/15124534374/why-encryption-bans-wont-work-brazil-governments-whatsapp-block-just-sends-users-to-other-encrypted-platforms.shtml.

Diffie, Whitfield, and Martin E. Hellman. 1976. “Multiuser Cryptographic Techniques.” *Proceedings of the June 7-10, 1976, National Computer Conference and Exposition on - AFIPS ’76*, 109. doi:10.1145/1499799.1499815.

Diffie, Whitfield, and Susan Landau. 2007. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Updated an. The MIT Press. https://books.google.nl/books?hl=en&lr=&id=nMY8yHaTQi4C&oi=fnd&pg=PR9&dq=Privacy+on+the+line:+the+politics+of+wiretapping+and+encryption&ots=DR0_KZxmhg&sig=HMoTJO0mxc0W9PCXaISNhloy3AA#v=onepage&q&f=false.

DIGITALEUROPE. 2016. “DIGITALEUROPE Views on Encryption.” http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2241&language=en-US&PortalId=0&TabId=353.

Eckstein, Barbara. 2015. “No Encryption Back Doors, Says EU Digital Commissioner.” *Computerworld.com*. http://www.computerworld.com/article/2924330/security0/no-encryption-back-doors-says-eu-digital-

commissioner.html.

EDRi. 2016. “Hungary: New Government Proposals Raise Concerns.” *EDRI.org*. https://edri.org/hungary-new-government-proposals-raise-concerns/.

Egberts, Martijn. 2016. “Tweet of 22 Aug 2016 08:24.” *Twitter.com*. https://twitter.com/MartijnEgberts1/status/767744247470628864.

elisa.com. 2016. “The Finnish Communications Regulatory Authority Grants Encryption Product Approval to a Mobile Communications Solution Created by Bittium, Digia and Elisa in the Bittium Tough Mobile Smartphone.” *Elisa.com*. http://elisa.com/press-releases/bulletin/?id=84346892661482&tag=corporate.elisa.com%3Apress.

Encryption Working Group. 2016. “Encryption Working Group Year-End Report.” http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/documents/114/analysis/20161219EWGFINALReport_0.pdf.

Europol, and ENISA. 2016. “On Lawful Criminal Investigation That Respects 21st Century Data Protection.” https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection.

Faeraas, Arild. 2014. “Sources: We Were Pressured to Weaken the Mobile Security in the 80’s.” *Aftenposten.no*. http://www.aftenposten.no/verden/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-98459b.html#.UtBeNpD_sQs.

Falkvinge, Rick. 2016. “Germany, France Demand Golden Key AND Strong Encryption Just When You Thought Politicians Had Clued in to Basic Reality.” *Privateinternetaccess.com*. https://www.privateinternetaccess.com/blog/2016/08/germany-france-demand-golden-key-strong-encryption-just-thought-politicians-clued-basic-reality/.

Farivar, Cyrus. 2016. “Feds to Court: Apple Must Be Forced to Help Us Unlock Seized iPhone | Ars Technica.” *Arstechnica.com*. http://arstechnica.com/tech-policy/2016/02/feds-to-court-apple-must-be-forced-to-help-us-unlock-seized-iphone/.

Feinstein, Dianne, and Richard Burr. 2016. “Encryption Without Tears - WSJ.” *Wsj.com*. http://www.wsj.com/articles/encryption-without-tears-1461798028.

France-Presse. 2016. “French Parliament Votes to Penalise Smartphone Makers over Encryption.” *Theguardian.com*. https://www.theguardian.com/technology/2016/mar/03/french-parliament-penalise-smartphone-makers-over-encryption.

Freedom House. 2015. “Estonia.” *Freedomhouse.org*. https://freedomhouse.org/report/freedom-net/2015/estonia.

———. 2016. “Freedom on the Net 2016.” *Freedom on the Net 2016*. https://freedomhouse.org/sites/default/files/FOTN 2016 Malaysia.pdf.

Froomkin, Dan. 2015. “Signs Point to Unencrypted Communications Between Terror Suspects.” *Theintercept.com*. https://theintercept.com/2015/11/18/signs-point-to-unencrypted-communications-between-terror-suspects/.

Gaj, K, and A Orlowski. 2003. “Facts and Myths of Enigma: Breaking Stereotypes.” *Advances in Cryptology-Eurocrypt 2003* 2656: 106–22. doi:10.1007/3-540-39200-9_7.

Gallagher, Sean. 2015. “What the Government Should’ve Learned about Backdoors from the Clipper Chip | Ars Technica.” *Arstechnica.com*. http://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-chip/.

Gassee, Jean-Louise. 2016. “The Dumb, Delusional US Senate Encryption Bill Is Everything Wrong with Tech Politics — Quartz.” *Qz.com*. http://qz.com/664104/the-dumb-delusional-us-senate-encryption-bill-is-everything-wrong-with-modern-politics/.

Gefen, David. 2000. “E-Commerce: The Role of Familiarity and Trust.” *Omega* 28 (6): 725–37. doi:10.1016/S0305-0483(00)00021-9.

Geller, Eric. 2016. “Top E.U. Network-Security Official Slams Proposals for Encryption Backdoors.” *Dailydot.com*. http://www.dailydot.com/layer8/encryption-backdoors-enisa-director-criticism-uk-france-us-crypto-wars/.

Gilbert, David. 2015. “David Cameron Preying on Our Fears after Charlie Hebdo Massacre with Encryption Ban Calls.” *Ibtimes.co.uk*. http://www.ibtimes.co.uk/cameron-preying-our-fears-after-charlie-hebdo-massacre-calls-encryption-ban-1483201.

Green, Matthew. 2016. “Is Apple’s Cloud Key Vault a Crypto Backdoor?” *Cryptographyengineering.com*.

https://blog.cryptographyengineering.com/2016/08/13/is-apples-cloud-key-vault-crypto/.

Greenberg, Andy. 2015. “Lockpickers 3-D Print TSA Master Luggage Keys From Leaked Photos | WIRED.” *Wired.com*. http://www.wired.com/2015/09/lockpickers-3-d-print-tsa-luggage-keys-leaked-photos/.

———. 2016a. “Meet Moxie Marlinspike, the Anarchist Bringing Encryption to All of Us.” *Wired*. https://www.wired.com/2016/07/meet-moxie-marlinspike-anarchist-bringing-encryption-us/.

———. 2016b. “The Senate’s Draft Encryption Bill Is ‘Ludicrous, Dangerous, Technically Illiterate’ | WIRED.” *Wired.com*. https://www.wired.com/2016/04/senates-draft-encryption-bill-privacy-nightmare/.

Grondwet. 2016. “Wetten.nl - Grondwet - BWBR0001840.” Accessed January 23. http://wetten.overheid.nl/BWBR0001840/geldigheidsdatum_20-01-2016.

Grossman, Katie, Tracie Lo, and Lauren Schmetterling. 2006. “Cryptography in Ancient Civilizations.”

Hackett, Robert. 2016. “Dutch Government Backs Uncrackable Encryption.” *Fortune.com*. http://fortune.com/2016/01/05/dutch-government-encryption-no-backdoors/.

Hagemann, B Y Ryan, and Josh Hampson. 2015. “Encryption, Trust, and the Online Economy.” https://niskanencenter.org/wp-content/uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits.pdf.

Halsey, Ashley III. 2014. “The Secret Life of Baggage: Where Does Your Luggage Go at the Airport? - The Washington Post.” *The Washington Post Online*. https://www.washingtonpost.com/local/trafficandcommuting/where-oh-where-did-my-luggage-go/2014/11/24/16d168c6-69da-11e4-a31c-77759fc1eacc_story.html.

Hendrikman, Mark. 2016. “Nederlandse Inlichtendiensten Willen Versleutelde Communicatie ‘Breken.’” *Tweakers.net*. https://tweakers.net/nieuws/119139/nederlandse-inlichtingendiensten-willen-versleutelde-communicatie-breken.html.

Hildebrandt, Mireille. 2013. “Balance or Trade-off? Online Security Technologies and Fundamental Rights.” *Philosophy and Technology* 26 (4): 357–79. doi:10.1007/s13347-013-0104-0.

Horwitz, Josh. 2016. “WhatsApp’s Encryption Could Make It a Target of the Chinese Government.” *Qz.com*. http://qz.com/655778/whatsapps-encryption-could-make-it-a-target-of-the-chinese-government/.

Howell O’Neill, Patrick. 2016a. “Former NSA Chief Says U.S. Can Get around Encryption with Metadata, Argues against Backdoors.” *Dailydot.com*. http://www.dailydot.com/politics/michael-hayden-encryption-debate-clinton-bush/?tw=pl.

———. 2016b. “French Government Considers Law That Would Outlaw Strong Encryption.” *Dailydot.com*. http://www.dailydot.com/layer8/encryption-backdoors-french-parliament-legislation-paris-attacks-crypto-wars/.

———. 2016c. “French Secretary of State Says Encryption Backdoors Are ‘Not the Right Solution.’” *Dailydot.com*. http://www.dailydot.com/politics/france-encryption-backdoors-secretary-of-state-rejection-crypto-wars/.

Human Rights Watch. 2015. “Promote Strong Encryption and Anonymity in the Digital Age.” *Hrw.org*. https://www.hrw.org/news/2015/06/17/promote-strong-encryption-and-anonymity-digital-age-0.

Hungarian Spectrum. 2016. “The Orban Government’s Latest: Jail Sentences for Encryption Software Developers.” *Hungarianspectrum.org*. http://hungarianspectrum.org/2016/04/04/the-orban-governments-latest-jail-sentences-for-encryption-software-developers/.

Judiciary, Senate comittee of the. 2015. “Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy.” *Judiciary.senate.gov*. http://www.judiciary.senate.gov/meetings/going-dark-encryption-technology-and-the-balance-between-public-safety-and-privacy.

Kaye, David. 2015. “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.” http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx.

Kazhdan, Alexander (Ed.). 1991. *Oxford Dictionary of Byzantium*. Oxford University Press.

Kehl, Danielle, Andi Wilson, and Kevin Bankston. 2015. “Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s.” *New America*. https://static.newamerica.org/attachments/3407--125/Lessons From the Crypto Wars of the 1990s.882d6156dc194187a5fa51b14d55234f.pdf.

Kelly, Sanja, Mai Truong, Adrian Shahbaz, and Madeline Earp. 2016. “Silencing the Messenger: Communication Apps Under Pressure.” *Freedomhouse.org*. https://freedomhouse.org/report/freedom-net/freedom-net-2016.

King, Gary, Jennifer Pan, and Margaret Roberts. 2013. “How Censorship in China Allows Government Criticism but Silences

Collective Expression." *American Political Science Review* 107 (917): 326–43. doi:10.1017/S0003055413000014.

Koops, Bert-Jaap. 1999. "The Crypto Controversy."

———. 2013. "Overview per Country." *Cryptolaw.org*. http://www.cryptolaw.org/cls2.htm.

Krstic, Ivan. 2016. "Behind the Scenes with iOS Security." In . https://www.blackhat.com/docs/us-16/materials/us-16-Krstic.pdf.

Leite, Julia. 2016. "WhatsApp Ordered Blocked Again in Brazil Over Data Dispute." *Bloomberg.com*. https://www.bloomberg.com/news/articles/2016-05-02/facebook-s-whatsapp-blocked-again-in-brazil-over-data-dispute.

Levy, Steven. 2001. "Crypto." *Newsweek* 137 (3): 42–53. http://web.a.ebscohost.com.ezproxytest.leidenuniv.nl:2048/ehost/delivery?sid=fa5fd37c-e00d-48d0-9812-77b8616a510c%40sessionmgr4010&vid=1&hid=4214&ReturnUrl=http%3A%2F%2Fweb.a.ebscohost.com%2Fehost%2Fdetail%2Fdetail%3Fsid%3Dfa5fd37c-e00d-48d0-9812-77b8616a.

Ling, Justin, and Jordan Pearson. 2016. "Exclusive: Canadian Police Obtained BlackBerry's Global Decryption Key | VICE News." *Vice.com*. https://news.vice.com/article/exclusive-canada-police-obtained-blackberrys-global-decryption-key-how.

Lomas, Natasha. 2016a. "Encryption under Fire in Europe as France and Germany Call for Decrypt Law." *Techcrunch.com*. https://techcrunch.com/2016/08/24/encryption-under-fire-in-europe-as-france-and-germany-call-for-decrypt-law/.

———. 2016b. "Facebook Has Funds Frozen in Brazil in Another WhatsApp Encrypted Data Dispute." *Techcrunch.com*. https://techcrunch.com/2016/07/01/facebook-has-funds-frozen-in-brazil-in-another-whatsapp-encrypted-data-dispute/.

Luiijf, Eric, Kim Besseling, and Patrick De Graaf. 2013. "Nineteen National Cyber Security Strategies." *International Journal of Critical Infrastructures* 9 (1/2): 3. doi:10.1504/IJCIS.2013.051608.

Machkovech, Sam. 2016. "Obama Weighs in on Apple v. FBI: 'You Can't Take an Absolutist View.'" *Arstechnica.com*. http://arstechnica.com/tech-policy/2016/03/obama-weighs-in-on-apple-v-fbi-you-cant-take-an-absolutist-view/.

Masnick, Mike. 2016a. "French Government Wants A 'Global Initiative' To Undermine Encryption And Put Everyone At Risk." *Techdirt.com*. https://www.techdirt.com/articles/20160811/17370035220/french-government-wants-global-initiative-to-undermine-encryption-put-everyone-risk.shtml.

———. 2016b. "Putin Says All Encryption Must Be Backdoored in Two Weeks." *Techdirt.com*. https://www.techdirt.com/articles/20160708/07535134919/putin-says-all-encryption-must-be-backdoored-two-weeks.shtml.

McCarthy, Kieren. 2016. "UK's New Snoopers' Charter Just Passed an Encryption Backdoor Law by the Backdoor." *Theregister.co.uk*. http://www.theregister.co.uk/2016/11/30/investigatory_powers_act_backdoors/.

Menn, Joseph. 2014. "Exclusive: NSA Infiltrated RSA Security More Deeply than Thought - Study." *Reuters.com*. http://www.reuters.com/article/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331.

Miltenburg, Olaf van. 2015. "Open Encryptieprojecten Krijgen Half Miljoen Euro van Nederlandse Overheid." *Tweakers.net*. https://tweakers.net/nieuws/106723/open-encryptieprojecten-krijgen-half-miljoen-euro-van-nederlandse-overheid.html.

Ministere de L'Interieure. 2016. "Initiative Franco-Allemande Sur La Securite Interieure En Europe." *Interieur.gouv.fr*. http://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Initiative-franco-allemande-sur-la-securite-interieure-en-Europe.

Modderkolk, Huib. 2016. "Dreiging Is in Jaren Nog Niet Zo Groot Geweest." *De Volkskrant*, September 17. http://www.volkskrant.nl/4378383.

Moody, Glyn. 2016. "Dutch Government: Encryption Good, Backdoors Bad." *Arstechnica.com*. Accessed December 25. http://arstechnica.com/tech-policy/2016/01/dutch-government-encryption-good-backdoors-bad/.

———. 2015. "China's New Anti-Terror Law: No Backdoors, but Decryption on Demand." *Arstechnica.com*. http://arstechnica.com/tech-policy/2015/12/chinas-new-anti-terror-law-copies-uk-no-backdoors-but-decryption-on-demand/.

———. 2016a. "Russian ISPs Will Need to Store Content and Metadata, Open Backdoors." *Arstechnica.com*. http://arstechnica.com/tech-policy/2016/06/russias-new-spy-law-calls-for-metadata-and-content-to-be-stored-plus-

crypto-backdoors/.

———. 2016b. “Russian Spies Claim They Can Now Collect Crypto Keys - but Don’t Say How.” *Arstechnica.com*. http://arstechnica.com/tech-policy/2016/08/russian-spies-say-they-are-able-to-collect-crypto-keys-but-dont-say-how/.

Olander, Torben. 2013. “In Denmark, Online Tracking of Citizens Is an Unwieldy Failure.” *Techpresident.com*. http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy.

Parsons, Christopher, and Tamir Israel. 2015. “Canada’s Quiet History of Weakening Communications Encryption.” *Citizenlab.org*. https://citizenlab.org/2015/08/canadas-quiet-history-of-weakening-communications-encryption/.

Pelgrim, Christiaan, and Annemarie Kas. 2015. “Nieuwe Wet Geeft Inlichtendiensten Meer Bevoegdheden.” *Nrc.nl*. https://www.nrc.nl/nieuws/2015/07/02/nieuwe-wet-geeft-inlichtingendiensten-meer-bevoegdheden-a1415042.

Peterson, Andrea, and Ellen Nakashima. 2015. “Obama Administration Explored Ways to Bypass Smartphone Encryption.” *Washingtonpost.com*. https://www.washingtonpost.com/world/national-security/obama-administration-ponders-how-to-seek-access-to-encrypted-data/2015/09/23/107a811c-5b22-11e5-b38e-06883aacba64_story.html?utm_term=.19cd91195eca.

Pierson, P. 1996. “The New Politics of the Welfare State.” *World Politics* 48 (2): 143–79.

Prakash, Pranesh, and Japreet Grewal. 2015. “How India Regulates Encryption.” *Cis-India.org*. http://cis-india.org/internet-governance/blog/how-india-regulates-encryption.

Prisco, Giulio. 2015. “Estonian Government Partners with Bitnation to Offer Blockchain Notarization Services to E-Residents.” *Bitcoinmagazine.com*. https://bitcoinmagazine.com/articles/estonian-government-partners-with-bitnation-to-offer-blockchain-notarization-services-to-e-residents-1448915243.

Privacy International, and IT-Political Association of Denmark. 2015. “The Right to Privacy in Denmark.” https://www.privacyinternational.org/sites/default/files/UPR_Turkey.pdf.

Reback, Gedalyah. 2016. “5 EU States Demand Better Police Freedoms to Break Encryption as UK Implements Surveillance Law.” *Geektime.com*. http://www.geektime.com/2016/11/26/5-eu-states-demand-better-police-freedoms-to-break-encryption-as-uk-implements-surveillance-law/.

Reitman, Rainey. 2016. “Security Win: Burr-Feinstein Proposal declared ‘Dead’ for This Year.” *Eff.org*. https://www.eff.org/deeplinks/2016/05/win-one-security-burr-feinstein-proposal-declared-dead-year.

Reuters. 2016. “China’s Huawei Backs Apple in Fight over Encryption.” *Fortune.com*. http://fortune.com/2016/02/21/chinas-huawei-backs-apple/.

Schellevis, Joost. 2016. “OM: Versleutelde Diensten Als WhatsApp Steeds Groter Probleem.” *Nos.nl*. http://nos.nl/artikel/2127446-om-versleutelde-diensten-als-whatsapp-steeds-groter-probleem.html.

Schneier, Bruce. 2015. “TSA Master Keys - Schneier on Security.” *Schneier.com*. https://www.schneier.com/blog/archives/2015/09/tsa_master_keys.html.

———. 2016. “Michael Hayden and the Dutch Government Are against Crypto Backdoors.” *Schneier.com*. https://www.schneier.com/blog/archives/2016/01/michael_hayden_.html.

Schneier, Bruce, and Kathleen Seidel. 2016. “A Worldwide Survey of Encryption Products” 7641: 1–23.

Schoen, Seth. 2016. “Thinking About the Term ‘Backdoor.’” *Eff.org*. https://www.eff.org/deeplinks/2016/03/thinking-about-term-backdoor.

Security.nl. 2016. “EU-Voorzitter Slowakije Wil Encryptie Met Lidstaten Bespreken.” *Security.nl*. https://www.security.nl/posting/476718/EU-voorzitter+Slowakije+wil+encryptie+met+lidstaten+bespreken.

Soeteman, Krijn. 2016. “Rusland Wil Verplichte Backdoor in WhatsApp En Telegram.” *Tweakers.net*. https://tweakers.net/nieuws/112725/rusland-wil-verplichte-backdoor-in-whatsapp-en-telegram.html.

Specter, Michael A. 2016. “Apple’s Cloud Key Vault, Exceptional Access, and False Equivalences.” *Lawfareblog.com*. https://www.lawfareblog.com/apples-cloud-key-vault-exceptional-access-and-false-equivalences.

Steur, Van der, and Kamp. 2016. *Kabinetsstandpunt Encryptie*. https://www.rijksoverheid.nl/documenten/kamerstukken/2016/01/04/tk-kabinetsstandpunt-encryptie.

Stone, Jeff. 2016. “Encrypted WhatsApp Blocked In Brazil, Telegram Downloads Explode.” *Ibtimes.com*. http://www.ibtimes.com/encrypted-whatsapp-blocked-brazil-telegram-downloads-explode-2229970.

Stupp, Catherine. 2016a. “EU Cybersecurity Agency Slams Calls for Encryption Backdoors.” *Euractiv.com*. https://www.euractiv.com/section/digital/news/eu-cybersecurity-agency-slams-calls-for-encryption-backdoors/.

———. 2016b. “Five Member States Want EU-Wide Laws on Encryption.” *Euractiv.com*. http://www.euractiv.com/section/social-europe-jobs/news/five-member-states-want-eu-wide-laws-on-encryption/.

Swire, Peter, and Kenesa Ahmad. 2012. “Encryption & Globalization.” *The Columbia Science & Technology Law Review* XIII: 416–81. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602.

Tait, Matt. 2016. “Pandora’s Cloud Key Vault.” *Medium.com*. https://medium.com/@pwnallthethings/pandoras-cloud-key-vault-204498fd125d#.1uucea8zi.

The Law Library of Congress. 2016. “Government Access to Encrypted Communications.” https://www.loc.gov/law/help/encrypted-communications/gov-access.pdf.

Thomson, Iain. 2016. “French Say ‘Non, Merci’ to Encryption Backdoors • The Register.” *Theregister.co.uk*. http://www.theregister.co.uk/2016/01/15/france_backdoor_law/.

Travel Sentry. 2016. “How-It-Works.” Accessed January 17. http://www.travelsentry.org/index.php?option=com_content&view=article&id=47&Itemid=53&lang=en.

“Travel Tips | Transportation Security Administration.” 2016. Accessed January 17. https://www.tsa.gov/travel/travel-tips.

Valero, Jorge. 2016. “Ansip: ‘I Am Strongly against Any Backdoor to Encrypted Systems.’” *Euractiv.com*. https://www.euractiv.com/section/digital/interview/ansip-i-am-strongly-against-any-backdoor-to-encrypted-systems/.

van der Kroft, Daphne. 2016. “Bits of Freedom Biedt Bertholee Cursus Grondrechten Aan.” *Bof.nl*. Accessed December 22. https://www.bof.nl/2016/09/18/bits-of-freedom-biedt-bertholee-cursus-grondrechten-aan/#donationOverlay.

van der Steur, G.A., and H.G.J. Kamp. 2016. “Cabinet’s View on Encryption.” https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/nl-cabinet-position-on-encryption.

van Voorst, Sander. 2016. “Tweede Kamer Stemt Voor Behoud Sterke Encryptie.” *Tweakers.net*. https://tweakers.net/nieuws/116397/tweede-kamer-stemt-voor-behoud-sterke-encryptie.html.

Vance, Molins, Leppard, and Zaragoza. 2015. “When Phone Encryption Blocks Justice - The New York Times.” *The New York Times Online*. http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html?_r=0.

Verhoeven, Kees, Marijn van Vliet, Nick Mastenbroek, Myrthe van Dieijen, Dick van Egmond, and Ouke Arts. 2016. “Techvisie D66.”

Vermeij, Azmani, and Franke. 2015. “Raad Voor Vervoer, Telecommunicatie En Energie; Verslag van Een Algemeen Overleg;”

Weaver, Nicholas. 2016. “NSA and the No Good, Very Bad Monday.” *Lawfareblog.com*. https://www.lawfareblog.com/very-bad-monday-nsa-0.

Weitzner, Daniel J. 2016. “The Encryption Debate Enters Phase Two.” *Lawfareblog.com*. https://www.lawfareblog.com/encryption-debate-enters-phase-two.

Wolff, Josephine. 2016. “What We Talk about When We Talk about Cybersecurity : Security in Internet Governance Debates.” *Internet Policy Review* 5 (3): 1–13. doi:10.14763/2016.3.430.

Yaschenko, V. V. 2002. *Cryptography: An Introduction*. American Mathematical Soc. https://books.google.com/books?hl=en&lr=&id=NZPxBwAAQBAJ&pgis=1.

Zaske, Sara. 2015. “While US and UK Governments Oppose Encryption, Germany Promotes It. Why?” *Zdnet.com*. http://www.zdnet.com/article/while-us-and-uk-govts-oppose-encryption-germany-promotes-it-why/.

Zenger, Rejo. 2016. “Stel de AIVD Doorbreekt Versleuteling. Wat Dan?” *Bof.nl*. https://www.bof.nl/2016/12/18/stel-de-aivd-doorbreekt-versleuteling-wat-dan/.

Zetter, Kim. 2016. “Apple’s FBI Battle Is Complicated. Here’s What’s Really Going On.” *Wired.com*. https://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/.