Exploiting Cyber Crisis

In the context of the Dutch cyber crisis management

Universiteit Leiden

Overview

Title:	Exploiting Cyber Crisis in the context of the Dutch cyber crisis management
Assignment:	Master thesis
Date:	09/08/2017
Word count:	27.444
Author:	Rick Sauer
Student number:	1752111
Program:	MSc Crisis and Security Management
Faculty:	Governance and Global Affairs
University:	Leiden University, campus The Hague
Supervisor:	dr. J. (Jaap) Reijling
2nd reader:	dr. S.L. (Sanneke) Kuijpers

Foreword

Before this research commences, I wish to express my gratefulness to a few people. First, I wish to thank my parents, who have supported me throughout the process of this thesis. My gratitude goes out to prof. dr. Paul Ducheine and the other researchers at the NLDA for facilitating this thesis through an internship and for inspiring me on many occasions. Furthermore, I owe David van Duren my appreciation for his help in finding respondents for this research. Finally, I wish to thank my supervisor, dr. Jaap Reijling, for his clear comments and for his fair, to-the-point critiques.

-President of the U.S. on 'the cyber' (Trump, 2016).

"You know cyber is becoming so big today. It is becoming something that a number of years ago, a short number of years ago, wasn't even a word. ***Now the cyber is so big****. You know you look at what they're doing with the Internet, how they're taking recruiting people through the Internet. And part of it is the psychology because so many people think they're winning. And you know there is a whole big thing. Even today's psychology, where CNN came out with a big poll, their big poll came out today that Trump is winning. It is good psychology."*

Abstract

This thesis is an explorative study to the conceptual framework of crisis exploitation, created by Boin, 't Hart, and McConnell (2009), in relation to crises in the cyber domain. In addition to being a new, and in this context unstudied, domain, the characteristics of the cyber domain potentially affect the mechanisms of crisis exploitation. This is researched through a case study in the context of the cyber security policy domain in the Netherlands. For this purpose, two different types of cyber crises are studied: the Diginotar hack and the Snowden revelations. In the subsequent content analysis of inquiry documents, media reports, and interviews, evidence is found that in both cases, actors have made exploitation attempts. Furthermore, evidence indicates that the characteristics of the cyber domain have some influence on the mechanisms of crisis exploitation, most notably through the volatility of its spheres of impact, and the occurrence of an additional, online, arena. Supported by the exponential growth in cyber crisis cases that occurred during the writing process, this thesis highly recommends further study to apply the model to additional cases.

Key words: Security Studies, Crisis Management, Crisis Exploitation, Cyber Crisis

Table of contents

List of figures

List of abbreviations

AIVD	Algemene Inlichtingen- en Veiligheidsdienst	(NL)
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence	
CERT-BUND	Computer Emergency Response Team Bundesverwaltung	(GE)
CSBN	Cyber Security Beeld Nederland	(NL)
CSR	Cyber Security Raad	(NL)
DCS	Directie Cyber Security	(NL)
ENISA	E.U. Agency for Network and Information Security	(EU)
GOVCERT	Government Computer Emergency Response Team	(NL)
IRB	Incident Response Board	(NL)
IVJ	Inspectie Veiligheid and Justitie	(NL)
MIVD	Militaire Inlichtingen- en Veiligheidsdienst	(NL)
NATO	North Atlantic Treaty Organization	
NCSC	Nationaal Cyber Security Center	(NL)
NCSS	Nationale Cyber Security Strategie	(NL)
NSA	National Security Agency	(US)
OVV	Onderzoeksraad voor Veiligheid	(NL)
PKI	Public Key Infrastructure	

1. Introduction

A crisis is the biggest challenge a policymaker can face. Under the pressure of time, threat and uncertainty, crises can have the worst outcomes imaginable. Undesirable as they may seem, a group of authors argue that crises simultaneously create opportunity (Rosenthal, Boin & Comfort, 2001; Alink, 2006; Ulmer, Sellnow & Seeger, 2013) - opportunity to either reform or reinstate the status quo. Fundamental to this theory is the thought that crises create a window of opportunity to affect policy, which can take the form of changing existing policies or consolidating conventional policy. Some crisis managers succeed in shielding policy from destabilization and radical change in the aftermath of a crisis, whilst protecting the policymakers and institutions responsible from reputation losses and sanctions. Vice versa, a crisis can be used to push through policy that seemed unachievable before. It can break careers, or even call into question the entire institutional integrity of a field. An example of radical change following a crisis is the extensive tightening of gun control following the 1996 Port Arthur shooting in Australia. In contrast, a recent example of a crisis being used to consolidate the status quo are the actions undertaken by the Turkish government after the failed coup d'état that aimed to overthrow Recep Tayyip Erdoğan. Eventually, the momentum of this crisis was also used to push through institutional change, in the form of a constitutional shift from a parliamentary to a presidential system. The coup d'état crisis provided Erdoğan the opportunity to further strengthen his government's hold over the republic. Both examples illustrate a phenomenon: crises can be 'exploited'. If practiced well, this can be an extremely valuable policy tool, and it gives leaders of government and opposition reason to be both fearful and hopeful (Boin, 't Hart, & McConnell 2009: 101).

The field of *cyber security* has grown towards significance. Over time, technological developments have led to an information revolution, causing modern societies to digitalize and become dependent on the many aspects the domain – known as cyberspace – encompasses. This dependence is the main cause for the current need to secure this new domain; i.e. cyber security. In terms of security, the domain faces many threats. The entire array of actors is currently struggling with a response to new forms of crime, warfare and, relevant for this study, crises. Cyber crises are a phenomenon that increasingly occurs in policy documents, journalistic items, and international diplomacy, and this increase has been ongoing for at least three decades (Warner, 2012). Most recently, the Wannacry malware attack caused a crisis when it held hospitals, shipping firms, telecom companies and others 'ransom' through file encryption, effectively disabling critical functions (Washington Post, 2017). Once again, the

destructive potential of cyber crises was observable. Many policymakers have acknowledged this, and, in response, the cyber domain has increasingly been adopted in the regular crisis and security response structures. For example, cyber is now seen as the fifth domain of security by the North Atlantic Treaty Organization (NATO), alongside space, land, water, and air.

Although the concept of a crisis has acquired a significant focus in practice, this cannot be said about the academic efforts on cyber crises. Very little progress has been made in defining cyber crises and elaborating on its consequences, despite many calls to include the cyber domain in conventional security studies (Nye, 2010; Kello 2013; Dunn-Cavelty, 2016).

This study anticipates the increased likelihood and impact of *cyber crises* and, in doing so, aims to contribute to solving the challenges they pose, or at least demonstrate how they can be, and may have been, used as a policy tool in governing the cyber domain. It furthermore advocates to prepare for this and will offer the required theoretical insight to do so, using theory that was the result of analysing this and other domains.

Before the study commences, it should be mentioned that its analysis takes place post-crisis. After a crisis occurred, its 'exploitation' should be regarded as a part of the general process of handling the aftermath. Academically this is known as the field of crisis management, which itself is one of the main themes in the broader field of security studies. At this point, the opportunistic value of a crisis and the field of cyber security are introduced, but how do they relate in practice and why does this matter? The answer lies in the process of crisis exploitation. *Crisis exploitation* is a concept introduced by Boin, 't Hart and McConnell (2009). In their article, they set out the lines of a theoretical framework for understanding the mechanisms of crisis exploitation. In an inductive analysis of fifteen crisis cases, they noted that despite their similarities, the cases showed significant variation in their consequences: some made political heads roll and caused profound policy change, and in contrast, other crises consolidated the position of those in charge and the policy they were responsible for. Examples include the crisis of 2005 hurricane Katrina, that caused severe damage to the position of George W. Bush and his administration, whilst in contrast, the 2002 Elbe flood crisis strengthened the position of Bundeskanzler Gerhard Schröder, propelling him towards electoral victory. Lacking a theoretical explanation to account for such variation, Boin, 't Hart and McConnell (2009) created the concept of crisis exploitation. This theory departs with understanding the aftermath of crises in the narrative of a *framing contest* between multiple actors with conflicting interests. These actors seek to explain a crisis and shape its consequences. In other words; they seek to exploit the crisis. Boin, 't Hart and McConnell define the process of exploitation as the

> "purposeful utilization of crisis-type rhetoric to significantly alter levels of political support for public office-holders and public policies" (2009: 83).

Ergo, crises can be exploited, and there is reason to believe that this process can have drastic consequences. Alongside its influence on political support, crisis exploitation can potentially account for a phenomenon that academics have struggled to explain: the occurrence, or absence, of policy change. In addition, the model may also have a role in explaining institutional reform (ibid.: 101). Based on these three implications, researching the model of crisis exploitation has strong academic value. As Boin et al. acknowledge (ibid.), further research on this model is required. In fact, the explanation that Boin et al. offer in the model of crisis exploitation is tentative and its conclusions preliminary. The authors note that further conceptual research on this model is required. A listing of recommendations includes the analysis of the crisis exploitation model in additional, and diverging, cases, as well as taking a separate look at the institutional effects of crises (ibid.).

Re-enter cyber crises to this equation. The premise of this study is that analysing the domain of cyber crises can provide further insight into the mechanisms of crisis exploitation, and it believes this for two sets of reasons. First, it answers the academic call for more and broader practical analysis of the model, through analysing a new domain and form of crisis that have not yet been studied in this regard. Secondly, the mechanisms of the crisis exploitation model may be compromised by the characteristics of the cyber domain. A large part of this model is based on the relative immobility of the "core community values and basic structures" of its spheres political support, policy change and institutional reform (ibid.: 83-84). However, in the cyber domain, these seem far less established. Particularly in policy, but also in terms of institutional reform, this domain seems far more volatile than the conventional domains on which the theory is based. This could be explained by the incipiency of the cyber domain; the domain develops quickly, and it seems likely that crises can expose vulnerabilities that lead to alteration. However, this could also be caused by the characteristics of the domain itself. Within the domain, there is a strong diffusion in actor relevancy (Nye, 2010). Issues with ownership and expertise in the cyber domain empower the private sector, meaning that the public sector might pull on far less of the strings that cause alteration in policy, political support and institutions - the impact spheres of crisis exploitation. This actor dynamic has already manifested itself within the governmental context of the Netherlands, as exemplified by the influential advisory council 'Cyber Security Raad', composed of 50% actors from the private sector, and the 'ICT Response Board', which is consulted during cyber crises and is composed of actors representing the private sector as well. In addition to the effect of the cyber domain

on the crisis exploitation components ‘crisis’. ‘actors’ and ‘impacts’, there is also a potential influence on the ‘arenas’ in which crisis exploitation takes place, all of which are further elaborated upon in chapter 2.2.3.

In sum, the key ingredients of this thesis are the academic cause to further study the preliminary model of crisis exploitation, and the societal cause to study the effects of crises in the cyber domain on governance. Do the mechanisms of crisis exploitation work in this new domain, and what does this mean for the model itself? This is a legitimate question, because the domain is not only new, but also encompasses characteristics that deviate from the domains on which the theory is based, which may have a compromising effect.

To gain substantiated insight in these causes and the effects of their interaction, this study conducts an explorative, in-depth analysis of two cyber crisis cases that have occurred in the public order of the Netherlands, and have strong internal variation in relation to each other: the Diginotar hack (2011) and the Edward Snowden revelations (2013). This variation is characterized in a typology that differentiates cyber crises in two groups; crises ‘through’, and crises ‘facilitated by’ the cyber domain, which is further accounted for in chapter 2.2.2.

By analysing the above, the study essentially tries to answer the question
‘Are the Diginotar Hack and the Edward Snowden revelations wittingly exploited in the context of the cyber security domain of the Netherlands, and if so, through which mechanisms?’.

This research question is central, and will be answered using the following structure. The theoretical section of this study, chapter 2, will commence with an in-depth explanation of the model of crisis exploitation, which includes a discussion of its context; the process of framing contests; and the mechanisms of the model, the three together constructing subchapter 2.1. Continuing, subchapter 2.2 will discuss the domain that is being applied to this model, the cyber domain, including a discussion of its characteristics; a definition of cyber crises; and an elaboration of its implications for the crisis exploitation model. The chapter is concluded with an analytical framework, chapter 2.3, in which the research question is further defined in the subquestions necessary to answer it, which are operationalized in the consecutive paragraphs. Chapter 3 discusses the methods used to analyse the data, whilst accounting for its sources. Chapter 4 consecutively applies these methods to both cases, structured through answering the subquestions required to answer the research question, which is concluded with a presentation of these results in terms of the results cross case. Concluding, chapter 5 will give meaning to answering the research question by providing contextual, academic and societal reflection. Finishing, this meaning is translated into policy recommendation and notes for further study.

2. Theory

The structure of the following chapter is tripartite: First, it explains its core theoretical model, the model of crisis exploitation. Secondly the context of cyber security is included in the equation. After a contextualization of the cyber domain and its outlying characteristics, and an elaboration of cyber crises, the potential implications of this domain for the theoretical model will be discussed. The last part brings the former two chapters together in a research question. This question is subsequently divided into research question, that correspond with the consecutive research themes that are operationalized in the final paragraph of this chapter.

2.1 Model of crisis exploitation

At the core of this research lie the mechanisms of the model of crisis exploitation. To fully explain these, its theoretical origins are elaborated upon, as well as the process of crisis exploitation, which Boin et al. see a contest of frames (2009:82).

2.1.1 Theoretical context of crises and crisis exploitation

To understand the concept of crisis exploitation, it is important to consider its theoretical origins. Like most of the theories used in the broader field of security studies, the theory of crisis exploitation as created and applied by Boin, 't Hart and McConnell (2009) has its roots in the field of public administration. More specifically, it is situated in the subject of studying policy change and reform. This subject that remains hard to explain until today and academia has yet to find a conclusive answer to it. Empirical analysis does find a relationship between crisis and reform. In fact, reform of policy appears to be nearly impossible under normal circumstances, without a disruptive event (Caiden, 1991; Wilsford, 1994; Shepsle, 2001). In regular circumstances, real reform is hard to push through, as old policies provide certainties, as there is a lack of urgency, and as there are many other subjects occupying the policymaker's agendas. These factors inevitably invoke hesitation in changing these agendas. After all, using a system that is not functioning optimally but is functioning nonetheless is a much safer option than taking a risk for reform. A crisis can change this situation.

Governance is portrayed as a pattern of long eras of stability intermitted by brief periods of conflict and uncertainty that put pressure on the dominant institutions, policies, and people. It is at these junctures that reform is most likely to happen, Baumgartner and Jones (1993) argue: when the 'equilibrium' is 'punctuated', i.e. their punctuated equilibria theory. The influence of crises on policy situations is also portrayed by Kingdon (1984). He argues that

crises have the potential to set the political agenda, for their disruptive character opens a "window of opportunity" (ibid.). Subsequently, this window of opportunity can be used to gain political momentum, potentially resulting in "the rotations of elites, revision of policies and the redesigning of institutions" (Boin, 't Hart, Stern and Sundelius, 2016: 133).

Regarding a crisis as an opportunity is something found throughout history and culture. For example, former U.S. president John F. Kenney used the it as a saying in a public address: "In the Chinese language, the word 'crisis' is composed of two characters, one representing danger and the other, opportunity" (1959). This is not entirely correct, but rather an etymological fallacy, as the symbol representing opportunity in the Chinese language is quite polysemous, having a more nuanced literal meaning. But nevertheless, the idea seems to resonate within contemporary politics. For example, Rahm Emmanuel, Barack Obama's Chief of Staff during the financial crisis, illustratively noted that "you never want a serious crisis to go to waste" (Wall Street Journal, 2008).

Figure 1: Simplified Chinese symbol for crisis, consisting of the symbol 'danger' and the symbol 'opportunity'

The academic world has adopted the concept too, many authors having discussed the opportunistic value of crises, leading to valuable academic contributions, including but not limited to Keeler (1993), Rosenthal, Boin & Comfort (2001), Alink (2006), Birkland (2006) Kuipers (2006), Ulmer, Sellnow & Seeger (2013). Within the broader theme of decision making, they have in common that they apply the insights of Cohen, March and Olsen (1972) who famously captured the phenomenon of decision making within the policy environment as

> ''a collection of choices looking for problems, issues and feelings looking for decision situations in which they might be aired, solutions looking for issues to which they might be the answer, and decision makers looking for work'' (1972:2).

The innovative part of this is the idea that decision making works the other way around: not with a problem as the point of departure, but with a solution as the point of departure. This solution – or issue – is looking for a way of applying itself. Cohen, March and Olsen thus observe a process of a collection of solutions and dubbed this the garbage can model. Crisis exploitation falls within this family of thought. Within the aftermath of a crisis, it looks at decision-makers seeking to exploit it with their own solutions (Boin et al., 2009: 82) - sometimes referred to as the political aftermath of crises (Boin, 't Hart, Stern and Sundelius,

2016). Before the way in which this works is explained, it is important to consider what is meant with the other core element of the theory: crises.

The term 'crisis' is broadly applied, and it is not always clear when something is a crisis and when not. In popular use, a disturbance is easily dubbed a crisis. Academics have tried to demarcate this term, some of them arguing that there is a "lack of consensus around the definition of crisis" (Roux-Dufort and Lalonde, 2013: 1). However, since this is an operational rather than a definitional complication, this study will not be affected by this lack of this consensus. Rather, it uses the popular definition drafted by Rosenthal, 't Hart and Charles, that aptly captures the meaning of the term 'crisis' as follows:

> "A crisis is a serious threat to the basic structures or fundamental values and norms of a social system, which, under conditions of time pressure and very uncertain circumstances, demands critical decision-making" (1989: 10).

Interpreting this definition; a crisis 'threatens' aspects of systems that have been certainties before the occurrence of this crisis. They are the critical junctures in the lives of these systems (Boin, 't Hart, Stern and Sundelius, 2016: 5). The above definition has seen various alternative, but very similar, formulations. However, three critical conditions are dominant in these definitions: crises are constituted by being a (1) threat, being (2) urgent, and by bringing along (3) uncertainty (Rosenthal, Boin, & Comfort, 2001; Rosenthal, 't Hart, & Charles, 1989). Combined they necessitate critical decision-making.

For unspecified reasons, the definition of crises that Boin et al. apply in their theory of crisis exploitation partially deviates from these components (2009). Rather, they define crises as: "events or developments widely perceived by members of relevant communities to constitute urgent threats to core community values and structures." (ibid.: 83-84). This definition includes a social component in *widely perceived*: the application of Thomas' theorem to define that crises 'are' a crisis, if they are 'believed to be' a crisis (ibid.). For methodological accountability, discussed in chapter 3, this thesis uses both above definitions. In this, it is valuable to consider when events or developments are *not* crises, or when events and developments that are not referred to as a crisis, in fact are. The following four concepts are most often confused, or interchangeably used, with crises: emergency, incident, disaster, and catastrophe. Firstly, an emergency. An emergency is not the same as a crisis. Within an emergency, only the time pressure component needs to be present. Likewise, and secondly, an incident does not need all the components necessary for a crisis but is rather interpreted as "All temporary and from the normal diverging events that result or could result in damaging consequences for security, health and/or environment" (ENISA, 2014: 26). Thirdly, a disaster

is an extreme situation with loss of life and severe, long term damage to property and infrastructure; a 'crisis with a bad ending' (Boin, 2005: 163). Finally, a catastrophe is a crisis to a superlative degree, having a "qualitative jump" over disasters, with important consequences in the sense of loss for a given collective, and unsettling a social structure (Quarantelli, 2005: 2).

In sum, it is important to realize that crises are social constructs that come in different shapes and sizes. What is regarded as a crisis can change over time, for example when a new domain such as cyberspace becomes relevant. The critical take-away is that crises are junctures in systems, that enable reform when they are politicized.

2.1.2 Framing contests and spheres of impact

With the theoretical origin and elaboration of crises in mind, the process of how these events of opportunistic value are politicized can now be discussed. As introduced, Boin, 't Hart, McConnell created a theoretical framework to analyse the exploitation of 15 crisis cases (2009). This theory resulted from an inductive study of crisis situations. In analysing the outcomes of their 15-crises database, they noticed a remarkable difference in the outcomes of comparable crises, especially in the form of support for office holders and degree of policy change. As an illustration, the 11/3 terroristic attacks in Spain resulted in a strong electoral loss for the prime minister's party, as well as a radical change in policy with the withdrawal of Spanish troops from Iraq. In contrast, the 9/11 terrorist attacks resulted in a surge in presidential and mayoral popularity, as well as radical change in policy. Based on the differing outcomes in their cases such as the above, Boin et al. concluded that between the independent variable of crises and the dependent variables of support for office holders and degree of policy change, a certain intermediating process takes place that can explain the differences in outcomes (2009). This process is what henceforth will be understood as crisis exploitation. In their own words, crisis exploitation can be defined as the

> "purposeful utilization of crisis-type rhetoric to significantly alter the levels of political support for officeholders and public policies" (Boin et al., 2009: 83).

In this definition, a linguistic demarcation is in order. Some actors are very successful at exploiting a crisis unwittingly. For example, the office-holder who objectively does everything in his or her power to combat a crisis, is sometimes highly rewarded. The crisis manager did his or her job well, and in doing so profited from the situation. However, this thesis argues that this is not the exploitation of a crisis. Inherent to the word exploitation is an awareness of a crisis' opportunistic value. Following this logic, a crisis is then only 'exploited' when this is

done wittingly. This reflects in the general definition of exploitation as 'making productive use of', or in other words, 'utilizing', a situation.[1] Although not specifically discussed in their article, Boin et al. seem to agree with this idea, as evidenced by the inclusion of the word *purposeful* in their definition of crisis exploitation (2009: 83).

Furthermore, this intermediating process of crisis exploitation is the 'utilization of crisis-type rhetoric'. Boin et al. argue that this occurs in a contest of frames following the respective crisis (2009: 83). Inherent to this contest is a conflict of interest between the contending actors. The respective contending actors compete to make their interpretation of the crisis, and what this should mean in terms of consequences, the dominant thought in the aftermath of the crisis. In other words, they try to 'frame' the crisis.[2] This is conducted in an almost game-like contest. Is the crisis an existential threat, caused by the negligence of the current policy elite? Or is the crisis merely an incident and should it be used to reinforce the existing policy framework? In other words, frames determine how a crisis is understood, which in its turn is crucial in what consequences the crisis will have.

Zooming in on the contest of frames, Boin et al. distinguish three possible frames that can be applied in the aftermath of a crisis: (I) *denial* of crisis, where a crisis is framed as nothing more than an unfortunate incident that should not have policy or political repercussions as a consequence; (II) the frame of a crisis as a *critical threat* to the status quo, where this is explained as a predisposition to defend those agents responsible for this status quo and their respective policies; or (III) a frame of crisis as a critical opportunity, where the current policies and those in office are being held responsible, and the argument is made that they should be reformed substantively or replaced in their entirety (ibid.: 84). The type I and II frames have been dominant in history. In historical perspective, crises were often regarded as 'an act of god', which resulted in denial of the crisis itself, arguing that they are but an inevitability of life. This falls within the category of type I frames. A second frame often observed in history does not deny the crisis, but rather acknowledges it as a critical threat. Within this frame, corresponding with type II, a logical response to the consequences of this threat is protecting the existing structures. This type of frame is seen, for example, when a country is being invaded by another country, and the society is mobilized to protect the status quo. The historical

[1] As included in Merriam-Webster's online dictionary.

[2] Boin et al. (2009) use Entman's following notion of framing: to frame is "to select some aspects of a perceived reality and make them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation" (1993: 52)

dominance of type I and II frames is largely determined by unquestioned state authority. Contemporary developments, including the emergence of cyberspace, however, change this situation. More often, crises are being regarded as indicators for a larger problem, which can only be solved through the reformation of structures. This has resulted in a shift towards type 3 frames, where crises are increasingly being framed as a critical opportunity. In sum, the situation of contest that ensues after a crisis is well described by Olsson, Nord and Falkheimer, as "rhetorical battles between pro- and counter-frames" between political actors (2015: 158). Some will try to interpret the crisis as a critical threat to the status quo, some will argue that it is a critical opportunity to change it.[3]

The impacts of crisis exploitation are observed in three spheres: the political, the policy and the institutional (Boin et al, 2009: 99).[4] These are the spheres that can either be reformed or consolidated. The political sphere centres around office holders, where oppositional forces may seek to blame incumbent office-holders for the occurrence of the crisis, or office-holders in turn may reject, deflect or diffuse responsibility. Essentially, it is about the consequences of clash between political government and opposition (ibid.: 88). An example of a crisis exploitation impact in the political sphere is the resignation of two Belgian ministers in the 1999 Dioxin Food Contamination crisis ('t Hart, 2009: 4-5).

The policy sphere is concerned with the degree of policy change. Essentially, it is about the consequences of clash between proponents of the regulatory and administrative status quo, and the advocates for change (ibid.: 88). If the goal of an actor in this game is to consolidate the current policy, it will adapt a type II frame and likewise, if the goal of the actor is to change policy, it will seek to exploit the crisis in a type III frame. An example of a crisis exploitation impact in the policy sphere are the major changes in water management legislation, and regulatory oversight practices following the 2000 Walkerton water contamination crisis in Canada ('t Hart, 2009: 7).

[3] There is a slight remarkability in the logic of using Thomas' theorem to define crisis as 'being a crisis' if they are 'believed to be a crisis' (Boin et al. 2009: 83), whilst regarding type I frames as viable options in a contest of frames (ibid.: 84). If an actor succeeds in making denial of crisis the dominant frame, Thomas' theorem poses that there is no crisis to begin with. This study therefore assumes that type I frames do not occur in the practice of crisis exploitation, but rather regards it as 'governance as usual'.

[4] Boin et al. (2009) exclude the third impact of crisis exploitation, institutional reform, from their subsequent theoretical analysis, but do include it in their empirical analysis (ibid.: 92; 101). In the recommendations for further studies, it is argued that future studies should to take a separate look at the institutional effects of crises, but it is not substantiated why this is not done in the original work.

The institutional sphere is the most fundamental and concerns the institutional character of an entire policy sector (Ansell et al., 2016). If a crisis challenges the institutional arrangement within a system, it is referred to as an institutional crisis (ibid.: 415). This is also defined as a situation where "the institutional integrity of a policy sector is at stake" (Boin and 'T Hart, 2000: 12). The term 'institution' is not always clearly defined in practice. It has multiple interpretations; therefore, a slight demarcation is in order. When this thesis uses the word 'institution', a public entity is meant. This can further be demarcated into "state or local government, or any department, agency, special purpose district, or other instrumentality [of it]", a legal definition as applied by Cremin (2011: 152). Reform can be further defined as an organizational make-over of the institution, that changes the nature of this institution, i.e. a fundamental reform. Following, 'institutional reform' can then be observed when a fundamental organizational makeover in a public entity is observed in the aftermath of a crisis. An example of a crisis exploitation impact in the institutional sphere is the sweeping domestic security reforms following the 9/11 attacks in the U.S.A., and the institutional reform in the flagship creation of a new Department of Homeland Security ('t Hart, 2009: 3-4).

The key with these spheres is that although they are demarcated in this set-up, it is very likely that there are spill-over effects between them (Boin et al. 2009: 101). Also, the assumed roles of, for example, oppositional and governmental actors do not pre-determine what the respective actor is trying to push for in the contest of frames. Oppositional actors do not necessarily push for type III frames, criticize incumbents, and plea for policy change or institutional reform, and the same is true for governmental actors vice versa. Following a crisis, an oppositional actor might, for example, employ a type III frame, pushing for political change, but not criticize the respective policy or institutions in place. It is necessary to distinguish between actors and their actions in the respective spheres. Therefore, the impacts should be regarded as multi-dimensional, and, hypothetically, all combinations between actors and impacts in the different spheres are possible.

2.1.3 Mechanisms of crisis exploitation

Up to this point, we know that crisis exploitation occurs in the aftermath of a *crisis*, where *actors* utilize crisis-type rhetoric in a contest of *frames*, to significantly alter the *impact* of the crisis in the spheres of political support, policy change, and institutional reform. Notice that this corresponds with the Boin et al. (2009) definition of crisis exploitation and, additionally, note that the *cursive* words are discussed in the previous subchapters. The missing components in understanding the model of crisis exploitation are the answers to the question: how does this

work in practice? To answer this, the remaining components of *arenas* in which crisis exploitation takes places, and *factors shaping actor propensities* should be discussed. These 'shape' the impacts of the crisis exploitation games in the respective spheres.

First, crisis exploitation of crisis principally takes place in two arenas: the *mass media* and *official inquiries* (Boin et al. 2009: 95).[5] What happens in these arenas affects greatly which, if any, binding conclusions will be drawn in the crisis' aftermath (ibid.).

Starting with the arena of mass media, before the model of crisis exploitation was drafted, the influence of mass media in the aftermath of a crisis was already noticed by other scholars (Seeger, Sellnow, Ulmer, 2003; Ulmer, Sellnow, & Seeger, 2007). Actors in the framing games must perform in this particular arena to "obtain or preserve political clout" (Boin et al. 2009: 95). Media is one of the 'boards' on which the game of exploitation is played. It is argued that proactive and professional performance in this arena is key in explaining actor credibility, and actor credibility in its turn appears to be essential for the level of success in framing a crisis (ibid.: 96). Based on their analysis, Boin et al. find that the more the media's crisis reporting and commentary emphasize exogenous interpretations of a crisis, the less likely it is that government actors will suffer negative political consequences in its aftermath, and vice versa (2009: 96). A point that should be considered is the overlap between actors and media, as in many political systems, media outlets can have strong cross-over interests with political actors and their constituencies, which in some cases goes as far as ownership of (or more subtitle forms of dominance over) the mass media, as, for example, was the case of former Italian prime-minister Silvio Berlusconi. One could argue that in these cases, access to the arena of media is compromised, which could render a real contest of frames, the core element of crisis exploitation, impossible to achieve. In this study however, it is assumed that media in liberal democracies, such as in the context of the Netherlands, are predominantly independent of political actors.

The other 'board' on which the game of framing is played is the arena of the inquiry. In one form or another, inquiry almost certainly follows in the aftermath of a crisis (Boin et al., 2009:97). In these inquiries, questions of blame are asked and answered, to a large variety of potential outcomes. It is suggested that the way in which these inquiries are managed is

[5] Boin et al. use the words 'arena' and 'sphere' interchangeably (2009). However, what is meant with these words varies: the words spheres/arenas are used to show the possible impacts of crises (p.83), but also represent the places in which the frame games take place (p.95). The lack of demarcation is somewhat confusing, therefore this thesis choses to use 'spheres' for the fields of impact (policy, political, and institutional) and 'arenas' for to indicate where the frame game takes place (mass media/official inquiry).

determinate for eventual consequences of these inquires (ibid.). It is observed that incumbents are more likely to successfully survive the game of crisis exploitation if they manage to have an 'expert' commission as the main locus of official inquiry into the crisis, as opposed to a political, often parliamentary, inquiry (ibid.:100).

Secondly, the course and outcomes of crises are also heavily influenced by the nature of the disturbance that triggers the crisis, known as the *situational factors*, and by how crises are situated in political time, known as *contextual factors* (Boin et al. 2009: 95). Together, these factors shape the actor propensities.

In situational factors, the nature of the respective crisis seems to have a crucial role in affecting the dynamics and impacts of crisis exploitation (ibid.: 98). Sometimes, the nature of a crisis is so compelling that blame games can be true no-brainers: it is very clear which people, policy or institutional set-up is responsible for a crisis. An example that Boin et al. offer are the "obvious" mistakes made by the public prosecutor in Belgium when "convicted child molester and rapist Marc Dutroux was not quickly and methodically investigated when children started disappearing in Belgium" (ibid.: 98). In other cases of crisis, this is not so obvious. It appears that the scope and dimension of a crisis can impose a script, meaning that in some cases, blame is so clear that a real 'contest' of pushing frames is not observed.

Finally, some contextual, or temporal, factors shape actor propensities within the crisis exploitation game. Boin et al. note two of them in particular (2009). First, it matters for the discussion on blame at which temporal point of an administration a crisis occurs. In general, the closer to an upcoming election a crisis occurs, the more likely it is that blame can be focused on incumbents (ibid.: 99). Secondly, it is also noted that the earlier a crisis occurs in the time of the actor's incumbency, the less likely he or she is to suffer in terms of political support, but the more likely he is to let a crisis change policy.

As a summary of the above findings, the following quote might be useful:

> "Oppositional forces are more likely to gain the upper hand when: (a) the crisis is widely perceived to have endogenous causes; (b) incumbents have spent a long time in office; (c) incumbents have recently been getting a good deal of 'bad press'; and (d) they manage to instigate or capitalize upon a 'political' (non-expert) inquiry" (Boin et al. 2009: 100).

2.2 Characteristics of the cyber domain

The second component of this study entails the domain of cyber security, in which both the studied cases are situated. Next to being a relatively new field of security, there is reason to believe that the characteristics of this particular field have a compromising effect on the mechanisms of crisis exploitation discussed in the previous chapter. This effect is explored in the following structure. First, the context of the field is discussed, arguing what is different in this field in comparison with conventional security fields. Secondly, it elaborates on what a crisis in this field looks like. Drawing from the conclusions in the previous subchapter, the implications these characteristics may have on the model of crisis exploitation are discussed in the concluding paragraph.

2.2.1 Cyber context

The subsequent component of a theory on cyber crisis exploitation entails the domain in which it takes place. This domain is frequently referred to as 'cyberspace'. Cyberspace has seen an exponential growth in significance in the 21st century, best illustrated by the central role that one of its key components – the internet – has acquired in contemporary societies. In parallel, the significance of keeping this domain safe and reliable has boomed. The sector concerned with this issue is called cyber security. A cyber crisis is an eruption within this sector.

Before elaborating upon the components of cyber security and crises, the broader phenomenon and context of cyberspace should be discussed. Contemporary as it may seem, cyberspace is the result of historical processes. These processes were ongoing for half a century before its salience was broadly recognized (Warner, 2012: 781). Ultimately, the growth of 'cyber' to what it is known as today, is enabled by 20th century technological advances on the way that information is stored and transmitted, also known as the "proliferation of information and communication technology" (Dunn-Cavelty, 2016: 401). Herein, 'information' is key, for it is the unit of measurement in the cyber domain (Nye, 2010: 1). This is similar to the way that currency is the unit of measurement of the economical domain, and the way that nuclear warheads are the unit of measurement in the nuclear security domain. Instant transmission of information has been possible since the invention of the telegram, but because of the development of cyberspace, this is now available for virtually everyone on the globe, through, for example, instant messaging applications. This has changed society in such a rigorous way that modern times are now often referred to as 'the information age', which is characterized by an "explosion of information" (Nye and Welch, 2007: 234).

Within this changed information society, the cyber domain has acquired a central role. The most visible components in this is the internet. In addition to this well-known phenomenon, a full definition of cyberspace spans its entire ecosystem. Definitions differ in accordance with their applications, but at least include its human and infrastructural components alongside its virtual component[6]. For example, cyberspace is thought about in terms of four layers: a physical layer of devices and cables; a logical layer of considerations and decisions such as net neutrality; a layer of information and data; and a human layer that gives meaning to the concept as such (Clark, 2010: 1-4). For the purposes of this thesis, the following simplified definition is sufficient: "cyberspace is the realm of computer networks (and the users behind them) in which information is stored, shared and communicated online" (Singer and Friedman, 2014: 12). The main takeaway is that cyberspace is a complex concept that has unconventional characteristics, and is therefore regarded as a domain of its own. As they challenge the traditional methods of crisis management, the most important of these characteristics of cyberspace are mentioned below.

First, the domain itself remains relatively new and dynamic. Prominent scholars claim that conclusions in cyber research are per definition provisional because the observed phenomena are still incipient, making the ways in which they could evolve difficult to predict (Kello, 2013: 38). It is not unlikely that a technological 'game changer' will redraw the lines on which the domain is currently constructed. This is an especially complicating factor within making policy, which is increased by the fact that the transition of the domain's control from the academic and private sector to the public sector has only become prominent in the last two decades (Chourci, 2014). This is an issue as much of the ownership and expertise required to make informed policy decisions and exercise control, remains in the first two sectors. Cyberspace is broadly accepted as a new domain of governance, but a comprehensive policy framework is not yet established. It is, rather, still in development.

Secondly, the emergence of the cyber domain has a reassigning influence on actor relevancy. Traditionally, security is known as state centric, but in the cyber domain, power is far more diverged between and within actors (Nye, 2010). This means that other actors such as in the private sector (between), or even an individual hacker (within), have far more capacity to exercise power in cyberspace, as compared to the traditional domains of security. The main causes for this are a low price of entry, the anonymity, and asymmetries in vulnerability within

[6] For an elaboration on the definitions of cyberspace, see Ottis and Lorents' (2010) contribution to *the Proceedings of the 5th International Conference on Information Warfare and Security* of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

cyberspace (ibid.). This is furthermore enhanced by the extreme interconnectedness within cyberspace, causing a new form of proximity that complicates concepts as jurisdiction, or even territorial sovereignty (Tsagourias, 2016). At this point, the extent of the above phenomenon is for example observed in the financial sector. In reaction to the global financial collapse in 2008, and the abuse of trust by financial institutions that surfaced, an anonymous academic released the whitepaper for bitcoin, the first digital currency (Nakamoto, 2008). New technologies, including the distributed ledger technology known as blockchain, were introduced. Important for this study is that this technology *distributes authority*, meaning that the core code decentralizes decision-making in its system to all participants, rather than centralizing it with an institution or person. Furthermore, it works peer-to-peer, with no intermediating parties in an environment that is borderless, neutral, and open to all that have access the internet (Antonopoulos, 2017). This systematically changes the concept of trust. Trust in institutions, persons and intermediaries is essential in the way the financial system works, but the case of digital currency proves that the cyber domain has the potential to fundamentally change this: technology might decentralize trust and authority.

The possibilities that technology enables as exemplified in the case above, and the ways in which this can potentially change contemporary society, leads scientists to characterize cyberspace as contested. This means that it is a space where the state actor is currently unable or unwilling to exert full authority (Naughton, 2001).[7] Scholars broadly agree that this has rigorous consequences on our notion of (international) security (Nye, 2010; Kello, 2013; Singer and Friedman, 2014; Dunn-Cavelty, 2015; Carr, 2016). In practice, policymakers concerned with this domain continuously face the question of 'moulding' cyber into conventional policy, or creating new, 'tailor-made' policy frameworks.

Following the components of the cyberspace definition above, cyber security can then be defined as the protection of the cyber domain, including the physical objects on which it relies, and those that operate in it (Von Solms & Van Niekerk, 2013). This term is interchangeably used with information security, but as Von Solms & Van Niekerk argue, this is incorrect, for information security only concerns protecting the asset of information, whereas cyber security additionally concerns the physical and human components related to it (2013). The field of cybersecurity is dominated by subjects such as cyber-attacks, cyber defence, and cyber warfare. An eruption of a threat in the form of a cyber crisis is, however, under-

[7] Also see Part V of Clunan & Trinkunas (2010).

researched. The following section of this thesis will elaborate upon what *is* known about cyber crises in theory and practice, which it will translate into a new definition for the phenomenon.

2.2.2 Defining cyber crises

Crises come in different shapes and sizes, but conditionally contain at least the elements threat, urgency, and uncertainty. In terms of cyber crises, there is no academic attempt accepted as a general definition, which makes sense because the subject has hardly been studied. However, it is not the first time that the characteristics of the cyber domain have caused a definitional problem. In practice, cyber crises have often been added as a subset in conventional crisis management structures (Boeke, 2016: 45). Operational units have targeted definitional problems by adding 'cyberspace' to a traditional definition on crisis. For example, ENISA, the European Union Agency for Network and Information Security, uses Boin et al. (2005) to academically define a crisis as "A serious threat to the basic structures or the fundamental values and norms of a system, which, under time pressure and highly uncertain circumstances, necessitates making vital decisions defines", and cyber crisis simply as a

> "serious threat to the basic structures or the fundamental values and norms of a system (in cyber space), which, under time pressure and highly uncertain circumstances, necessitates making vital decisions" (ENISA, 2014: 28).

This approach is, however, too parsimonious, and does not capture the true nature of the concept. The biggest issue with incorporating the new domain in the crisis management body of knowledge is its borders with the traditional fields. For example, when an earthquake hits a data centre, causing a loss of vital information or access to information, is the subsequent crisis a cyber crisis or a natural crisis? Or perhaps both, making the crisis transboundary (Boin, 2005). It is noted that the current forms of cyber crises management often are constructed as a subset within generic crisis management (Boeke, 2016: 45), even though these structures are sometimes insufficient for addressing them (ibid.: 3). Other fields have struggled with this question as well. For example, the field of crime. Within this field, Gordon and Ford (2006) tackle this problem by dividing cybercrimes into two categories: purely technical crimes (type I), such as viruses and worms, and traditional crimes that are facilitated through cyber means (type II), such as online harassment and extortion.

In drafting a definition for cyber crises, this study proposes to use this categorization as follows: cyber crises are *serious threats to the basic structures or the fundamental values and norms of a system, either taking place in cyberspace or facilitated through cyber means, which, under time pressure and highly uncertain circumstances, necessitate making vital*

decisions. The following study uses this definition to analyse a cyber crisis of both types: the Diginotar hack (type I) and the Snowden revelations (type II). In the empirical analysis, it will be substantiated why these events are considered cyber crisis cases.

2.2.3 Implications for the crisis exploitation model

With regards to the core components of the model of crisis exploitation (crises, actors, frames, arenas, factors, and impacts), the following four are different in relation to the original domains on which the crisis exploitation model was based, and might therefore be of influence for the way the model works in practice in the cyber domain. There are different forms of (1) crises, in the form of cyber crises; potentially other (2) actors are of relevance in the form of actors from the non-public sector; there is an additional (3) arena 'online' that requires some discussion; and finally, the spheres of (4) impact might be more volatile, as the status quo seems far less established within the cyber domain.

The different forms of crisis that come with the cyber domain are discussed previously.[8] In terms of implications for the model, little other than that it is a new form is crisis is yet known. Potentially, the scope and dynamics of cyber crisis will have implications on how crisis exploitation works, but generalizations will have to result from an empirical analysis.

What we do know about cyber domain is that there is a strong diffusion of relevant actors in comparison with traditional domains (Nye, 2010). Issues with ownership and expertise in the domain empower other actors than state actors, especially including actors from the private sector. This might mean that public actors are not be the only relevant participants in the game of crisis exploitation, as Boin et al. seem to assume (2009). Even if this is not seen in practice, it is very likely that the influence of, at least, the private sector in the aftermath of a crisis is of more significance in this domain than in other domains. In terms of the policy, political, and institutional sphere, government strategy in the Netherlands officially comprises 'private-public-partnerships', meaning that the private sector is closely involved in the traditionally public task of governance (NCSC, 2013:3). This inclusion seems to be extensive, judging from the fact that it has already been institutionalized, as exemplified by the influential advisory council 'Cyber Security Raad', composed of 50% actors from the private sector, and the 'ICT Response Board', consulted during cyber crises, which is composed of private sector actors as well.

[8] See introduction and chapter 2.2.2

There is something deviant going on in terms of the media arena. As discussed in chapter 2.1.3, media is one of the two most important channels through which the contest of frames takes place. In this, however, there is the historical need to use mass media to communicate a message, for example, through news outlets such as paper and television. However, with the occurrence of cyberspace, instant transmission of information and communication to constituencies has become possible for virtually everyone, at virtually no costs (Nye, 2010). An example is the use of social media services such as Twitter as means of mass communication. In the 2016 U.S. elections, the eventual winning candidate, exercised much of his political framing through this outlet. Essentially, this characteristic of cyberspace gives contenders in the frame games the option to cut out the media middle man. Even if this is done partially, it would mean that in the framework, another arena in which the contest of frames is practiced, is relevant than those defined by Boin et al. (2009: 95).

Finally, there might be a different dynamic in the cyber domain in terms of impacts. A large part of this model is based on the relative immobility of the "core community values and basic structures" of its spheres political support, policy change and institutional reform (ibid.: 83-84). However, in the cyber domain, these seem far less established. As Kello (2013) notices, the domain is still in an incipient phase, and this reflects on the impact spheres. Following the findings in the situational factors of chapter 2.1.3, the more established the status-quo is, the more likely it is that changes will occur in the aftermath of a crisis (Boin et al. 2009: 98). Therefore, it seems very likely that the impacts of crisis exploitation in the domain of cyber are far more volatile in comparison with conventional domain.

2.3 Analytical framework

The final subchapter of the theoretical framework concerns the analysis of the concepts in practice. It takes the core elements of the crisis exploitation model and discusses why and how these can be found in the practice of cyber crisis cases.

2.3.1 Actors

Crisis exploitation is practiced by actors. In order to gain insight in the mechanisms of crisis exploitation in cases in the cyber domain, it is elementary that the question 'which actors are contending in the aftermath of the respective crisis?' is answered.

Boin et al. distinguish actors per sphere of impact (2009). In the political sphere, concerned with the alteration of levels of political support, Boin et al. distinguish between 'incumbents', actors holding public office, and 'critics', actors criticising public office-holders

(2009: 89). In the policy sphere, concerned with keeping or changing the pre-crisis policy, Boin et al. distinguish between status-quo players, concerned with protecting policy from change, vs. change advocates, concerned with changing policy (Boin et al. 2009: 90). Actors in the institutional sphere are not distinguished. Therefore, since institutional reform overlaps with policy change (ibid.: 101), this research chooses to define those in a similar fashion: as either status quo advocates, or reform advocates. As discussed, these spheres are not mutually exclusive, but should, rather, be regarded as multidimensional, meaning that an actor can be a change advocate in one sphere, but a status quo player in another sphere.

Within the studied crises, actors can either be individuals or organizations. This thesis will regard any actor who employs crisis-type rhetoric (see following paragraph) in the aftermath of a crisis a contender in the exploitation game. In other words, actors participating in crisis exploitation are indicated by their attempts to interpret the crisis in its aftermath, occurring in the respective arenas discussed later in this chapter. As found in the previous subchapter, there is reason to believe that within the cyber domain private sector actors can have a strong influence in the crisis exploitation process. Therefore, special attention will be given to the sectoral background of the participants in the contest of frames following the studied crisis cases.

2.3.2 Frames

Actors try to 'make meaning' of crises by framing them. To gain insight in the mechanisms of crisis exploitation in cases in the cyber domain, it is therefore elementary that the question 'what type of frame are the contending actors trying to push?' is answered.

Previously, it was discussed that there are three types of frames, two of which are considered possible frames in this model: type II, framing a crisis as a critical threat to the status quo, and type III, framing a crisis as a critical opportunity. In order to indicate crisis exploitation in their research question, Boin et al. define it as the "purposeful utilization of crisis-type rhetoric […]" (2009: 83).[9] With this, the concept of framing is being operationalized as indicated by the crisis-type rhetoric used by the actors participating in the 'meaning-making' contest that ensues in the aftermath of a crisis. But what exactly does 'crisis-type rhetoric' mean, and how can it be found in practice?

[9] This definition is based on Entman's following notion of framing: to frame is "to select some aspects of a perceived reality and make them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation" (1993: 52)

The answer lies in the language used in the aftermath of the crisis. From this language, it can be deduced which frame is being pushed. According to Boin et al. this language can be found in the clash over two different characteristics of the crisis: its *significance*, in which the importance of the crisis is discussed, and its *causality*, in which blame for the crisis is discussed (Boin et al., 2009: 85-88). The clash over significance is characterized by the debate about whether the crisis is an incident or a symptom of there being something wrong. Actors either minimize, acknowledge, or maximize the significance of the event (ibid.: 85). The clash over causality is characterized by actors who blame the crisis on either endogenous or exogenous factors (ibid.:87).

Following this logic, frames are indicated in crisis-type rhetoric. Crisis-type rhetoric can be found by analysing the language used to discuss the causality and the significance of a crisis in its aftermath.

2.3.3 Arenas

But where can the language indicating crisis-type rhetoric be found? The contest of frames occurs in two, or perhaps more, arenas. To gain insight into the mechanisms of crisis exploitation in cases in the cyber domain, it is therefore fundamental that the question 'in which arenas was the exploitation of the crisis principally acted out?' is answered.
Boin et al. recognize two arenas in which the contest of frames occurs: in the mass media, and through official inquiry (2009: 95).

What is meant with mass media remains undefined in Boin et al. (ibid.). Therefore, the work of McCombs and Shaw is applied in this study, using their classic definition of mass media as: television, newspapers, and news magazines (1972: 178-179). Within this definition, only outlets with a significant market share are considered as 'mass'. As argued, the cyber domain has the potential to add an additional 'online' category to this taxonomy. It is important to realise that these are the platform on which the framing contest central to crisis exploitation occurs. The second arena of official inquiry occurs in two forms: political and expert-based. Political inquiries are any inquires made through official political institutions, such as parliament. Expert-based inquiries are any inquiries made through official oversight and other evolutional committees. Summarizing, the contest of frames is observable in official inquiries, parliamentary or expert-based, and through mass media outlets, either conventional or digital.

2.3.4 Situational and temporal factors

During the process of crisis exploitation, the way in which actors tend to behave – the actor propensities – are heavily influenced by situational and temporal factors. Therefore, to find out how the mechanisms of crisis exploitation work in cases in the cyber domain, it is crucial to answer the question 'what situational and temporal factors shaped the actor propensities?'.

As discussed, situational factors concern the nature of the disturbance that triggers the crisis. The question here is one of scope (Boin et al., 2009: 98-99). Is the crisis easily compartmentalized, meaning that it is occurring within one sector with little overlap with other sectors, or does the crisis span several governmental issues? Situational factors are indicated by the quantity of sectors it hits; therefore, the quantity of governmental sectors involved in the crisis aftermath should be analysed.

Secondly, temporal factors concern the question in what political time a crisis is situated. Political time is the distance to an upcoming election, and the time of the actor's incumbency. Both are indicated by months.

Based on the analysis of the characteristics of cyberspace, no evidence is found that within the cyber domain additional temporal and/or situational factors are of influence. Nonetheless, this will be considered as a possibility and taken a separate look at in the empirical analysis.

2.3.5 Impacts

> "Any theory of crisis exploitation therefore needs to capture not just the emergence of frames, but how the clash between them produces particular types of political and policy consequences" (Boin et al. 2009: 88).

Following the logic put forth, it is important to look at what has changed after a crisis, in relation to the situation before the respective crisis. Therefore, it is important to answer the question: 'what political, policy and institutional impacts of the crisis are observable?'.

Impact of crisis exploitation is the difference between the situation before and after the respective crisis. This is observed in the political, policy and institutional sphere, which should be given a separate look.

The difference between the situation before and after a crisis in the policy sphere is indicated by *policy change*. Actors try either to invoke policy change, or, to prevent it from happening. Boin et al. use Sabatier's (1999) taxonomy to categorize degrees of policy change. In this taxonomy, policy change is understood as having three levels of depth of change: deep

core; core; and secondary aspects. These categories are superlative to each other, the least amount of change being secondary aspects of the policy, while the most fundamental form of policy change is deep core change. It is not specified what indicates to which category impacts of a crisis belong. Rather, Boin et al. apply a "loose fashion", i.e. without the use of a formal content-analytic coding scheme (2009: 103). This study choses to use this taxonomy as well, but in a different way. If the policy situation after a crisis has seen technical, instrumental adjustments in regulation and implementation practices, but nothing more, it will be considered 'secondary' policy change. If the policy situation goes further than that, for example, through changing its goals, it will be considered 'core' policy change. The superlative to that, 'deep-core' policy change, will be considered present if institutional change occurs, as discussed below.

The impact of a crisis on political support can be categorized into three forms (Boin et al., 2009: 91-94): elite damage, which occurs when the blame of a crisis is successfully focussed to the officeholder; elite escape, which occurs when blame is diffused or displaced; and elite rejuvenation, which occurs when instead of blame there is support and praise for the officeholders (Boin et al., 2009: 91-94). This impact is admittedly hard to measure. Political support can be quantified, which is what happens during elections, or for example in approval rates. Approval research is sometimes conducted following crises, but this data remains hard to acquire, let alone compare. Boin et al. do use electoral results as indicators for political support (2009: 92-93) under the *ceteris paribus* assumption that all other factors remain the same. At this point, cyber crises do not have the scope to have substantive, let alone decisive, influence on electoral results. Therefore, this is not a good indicator for measuring political support. Having no alternative to this method within the viable research limitations, this study will instead interpret political support impacts in a loose fashion, but will remain very nuanced in drawing conclusions based on this impact.

The most deviant of the impacts of crisis exploitation is institutional reform. Boin et al. mention the significant effect that crises can have on institutional reform frequently (2009: 82; 99; 101), yet they choose not to include them in their analysis. They did this because the "complexities and nuances" of this variable "need to be capture more fully" (ibid.: 101), and leave this task as a recommendation for further research. Since the publication of the article, research on the effect of crises on institutional reform has been further developed and evolved.[10] In this research, the idea is that a crisis can be so profound that it questions the entire

[10] See for example Ansell, Boin and Kuipers (2016).

institutional integrity of a policy sector, not just the policy itself (Alink, Boin, and ’t Hart, 2001). This is superlative to policy change. When it occurs, intense criticisms on the basic institutional arrangements and assumptions result in a loss of legitimacy for the respective institution (Ansell, Boin and Kuipers, 2016: 415). This does not often occur, and when it occurs, it is hard to miss.

2.3.6 Research questions

The purpose of this chapter was to explore the way in which crisis exploitation works, and to academically predict what would happen if it is applied to the domain of cyber security. After the research methods are accounted for, this study will continue with this application to two cases of cyber crises in the context of the Dutch cybersecurity domain: the Diginotar Hack and the Edward Snowden revelations. Both cases will be subjected to the following, central research question (RQ):

> *Are the Diginotar Hack and the Edward Snowden revelations wittingly exploited in the context of the cyber security domain of the Netherlands, and if so, through which mechanisms?*

To answer this central question, subquestions corresponding with the core elements of the model of crisis exploitation should be answered on a case to case basis. These subquestion are (1) which actors are contending in the aftermath of the respective crisis?; (2) what type of frames and crisis-type rhetoric are the contending actors trying to push?; (3) in which arenas was the exploitation of the crisis principally acted out?; (4) what situational and temporal factors shaped the actor propensities? and (5) what impacts of the crisis are observable?

3. Research design

In this chapter, the methods and data used to answer the research question are accounted for. Chronologically, this is done through discussing the methodological design, an elaboration on the collection of data, notes on data analysis, and a discussion of the scientific repercussions of the chosen methods in terms of validity and reliability. In sum, this chapter answers the question where, and how, the empirical data analysed in this study is found and analysed.

3.1 Methodological design

This thesis is an explorative study to the model of crisis exploitation. There is an absence of validated theories and validated empirical data on the relatively new phenomenon of cyber crises, and, additionally, further research to the exploitation of crises is required. This research aims to develop new ideas and insights for the gap clarified above.

As explorative research is 'exploring' theoretical deficits, it is not commonly testing hypotheses or searching for causality. Rather it demarcates an existing theoretical framework and applies it, as for example occurs in this study, to a new domain, observing what this means for the mechanisms of the model in general. This study does that through an analysis of two cases of cyber crises in the context of the Netherlands. In scientific terms, this is referred to as a multiple-N case study, with an N of 2. Case studies are qualitative methods of research that analyse one, or a few, cases in an in-depth fashion, using data that is predominantly text based.[11] This is in sharp contrast with quantitative research methods, that mostly consist of large N-cross case analyses that are using number based data. In this research design, the major entity that is being analysed, referred to as the unit of analysis, is crisis exploitation. The objects on which information is collected, the units of observation, are actors, frames, arenas, factors, and impacts.

In the original model of crisis exploitation, the independent variable, often referred to as X, is a crisis. In the research question *Are the Diginotar Hack and the Edward Snowden revelations wittingly exploited in the context of the cyber security domain of the Netherlands, and if so, through which mechanisms?* this is parallel. Through the intermediating variable of crisis exploitation, indicated by actors, frames, arenas, and factors, the variation in the dependent variable of impact can be accounted for.

The two analysed cases differ on variables other than the dependent and independent, namely the type of cyber crisis as defined in paragraph 2.2.2: Diginotar being a type 1

[11] See Creswell (2013) and Gerring (2007).

'technical' cyber crisis, and the Snowden revelations being a type 2, 'facilitated' cyber crisis. This makes them suitable for a most different case study model (Gerring, 2007: 90). Both cases are representative of the larger population of cyber crises, and the variation between the cases makes them valuable for discovering how the mechanisms of crisis exploitation may or may not be affected by the characteristics of the domain. The selection of both cases should be further discussed.

In general, the research of crises is limited, for the simple reason that they are a rare occasion. The entire set of crises that fit the definition as established in paragraph 2.1.1, consists a 'few each year' globally, and thus forms a population that is hard to research using quantitative cross-case methods, that require a large N to draft valuable generalizations. Cyber crises, furthermore, are a subgroup *within* this population of crises, and the amount of cases suitable for research is therefore even further limited. In this subgroup, the cases have a high degree of variation in their characteristics. In scientific terms, this is referred to as a heterogeneous research population (Gerring, 2007: 50).

In the research question, the distinctive demarcation 'in the context of the Dutch cyber domain' is made. In other words, it narrows an already limited research population down even further. The reason why this is done originates from the research method it uses. Case studies require an in-depth analysis to internal mechanisms, and this research argues that a valuable contribution should therefore use data beyond what is available through open sources. Within the limits of this research, only data acquisition in the context of the Dutch cyber domain was feasible. As a consequence, in this model, there are too many factors that are not taken into account to use it for a direct generalization of the entire population of global cyber crises. This study therefore makes a circumstantial argument, meaning that its conclusions are limited regarding the respective empirical universe of cyber crises, but according to Gerring, this can have strong academic value nonetheless (2007: 57). Considerations on 'data availability' are further discussed in the following paragraphs.

Within the relatively new cyber security domain, the only undisputed cyber crisis in the context of the Netherlands, is the Diginotar crisis of 2011. Open source analysis and a specific question in the conducted interviews proved that there is some discussion on the question if the second case, the Snowden revelations of 2013, was a crisis situation. This paper argues that it is, based on its compliance with all the elements of crises as defined in paragraph 2.1.1: it has all the vital components of threat, uncertainty and urgency. This will be further substantiated in paragraph 4.2.1. Based on the research conducted in this study, it furthermore appears that just a few other cyber incidents in the context of the Netherlands can arguably compete for the

categorization ‘cyber crisis’. The most notable cases being the 2011 series of leaks dubbed Lektober, the 2013 KPN hack, and the 2013 DDOS attacks targeting the public sector.[12] However, due to its large in-case variation in comparison with the Diginotar case, which makes the research of both analytically valuable and suitable for a most-different case study model, the Snowden case was selected.

3.2 Data collection

The empirical research that ensues is an analysis of multiple quantitative, text-based, data sources. These sources can be categorized into the categories open source data, and interview data. ‘Open source data’ consists of all the relevant non-academic sources that are publically available, originating from parliamentary inquiries, evaluation reports (by the public and the private sector), and journalistic items. The inquiries and evaluation reports are collected using the search engine for governmental documents ‘Overheidsdocumenten’, accessible through the general website of the government of the Netherlands. The journalistic items are collected through the search engine LexisNexis, that provides a conclusive database on the mainstream news outlets in the Netherlands. In one instance – (‘t Hart, 2009) – a document was irretrievable, necessitating consultation of the internet archive, through ‘WayBackMachine’. The ‘interview data’ category consists of the transcripts of the interviews that are conducted with experts in the field. These experts have a close professional association with the cases: they were all professionally associated with the aftermath of both the Diginotar and the Snowden Revelations crises.[13] The interviews of respondents A and B are fully transcribed, whereas due to its length, the interview with respondent D is it is not fully transcribed, but rather summarized to the respective interview questions. With the exception of the interview with respondent C, links to the full audio files of the interviews are available in the appendix

[12] During the writing of this thesis, two potentially relevant cases surfaced in a very short period of time: the Wannacry ransomware attacks in May 2017, and the related Petya ransomware attacks of June 2017. Especially the Wannacry ransomware attacks invoked a strong crisis-type situation, and discussion on existing policies in its aftermath. Unfortunately, the timing of these cases made it impossible to include them in this study, other than through mentioning them in the final chapter.

[13] The interviews conducted made use of a standardized, open ended set of questions, that can be found in Appendix B. The respective interview questions diverged from this set question on occasion, in order to provide clarity and/or a more in-depth answer to the respective question. Continuing, the conducted interviews were processed into literal transcripts, that were used as ‘unique data’ in the empirical analysis of the cases.

for verification purposes. Respondent C did not allow the interview to be recorded, but did allow the publication of the notes the researcher made during the interview. [14]

3.3 Data analysis

Data originating from open sources and interviews are analysed considering their academic point of departure, as provided in chapter 2 of this thesis. The data originating from the interviews contains ready to be used data, and the data coming from academic sources is acquired through literature review, but the data originating from open sources requires further research steps to be of value for the empirical analysis of this thesis. This is done through a content analysis: a research technique that produces replicable and valid inferences by interpreting and coding textual material through a systematic evaluation of text data. This is done through the construction of a coding scheme, or tree, wherein the applied codes are categorized. All the open source documents are coded using this coding scheme, found in figure 2. A software tool, MaxQDA version 12, is used for organized coding and provides the standardized overviews and outputs as seen in the chapter 4.

Figure 2: coding scheme

Code System		
Codes	Subcodes	Description
1. Actor		Those actors participating in the contest of frames, or exploitation game, following the crisis. This includes any actor (individual or organization) who employs crisis-type rhetoric (either on crisis significance or causality).
	Incumbent	
	Critic	
	Non-public actor	
2. Crisis type rhetoric and frames		The language in the aftermath of the crisis used to provide interpretations of its causality (endogenous or exogenous) and significance (incident or a symptom). This language is used to frame the crisis as either a critical threat (type II) or a critical opportunity (type III)
	Causality	
	Significance	
	Critical threat to status quo	
	Critical opportunity	

[14] Correspondence with both the respondent and this thesis' supervisor is available upon request for validation.

3. Arena of exploitation		The medium in which the contest of frames is exercised. Either through official inquiry (parliamentary or expert-based) or the mass media (conventional and/or digital)
	Official Inquiry	
	Media	
4. Actor propensities as result of factors		The factors relevant at the time the crisis takes place linked to the propensities of actors. These factors can either be situational (amount of involved governmental sectors) and temporal (political time of incumbency and upcoming elections)
	Temporal factors	
	Situational factors	
5. Impacts		What has changed after a crisis, in relation to the situation before the respective crisis. This is observable in the spheres political (the direction of blame), policy, and institutional impacts (both in terms of secondary, core, or deep core changes)
	Institutional	
	Political	
	Policy	

Through the structural variation of sources, academic; interview; open source, the method of analysis accounts for possible discrepancies and contradictions in the data. This 'triangular' method furthermore informs its findings from multiple perspectives, which in its turn benefits the reliability of these findings.

Figure 3 provides an overview of all data used in the empirical analysis, categorizing them to case, source, and type, to account for the potential effect of cyber on the mechanisms of crisis exploitation. The way in which the sources are analysed differ per unit of observation (actors, frames, arenas, factors, and impacts). For actors, the study looks at the persons or organisations that frequently employ crisis type rhetoric. This is analysed through counting and analysing the occurring 'players' in the contest of frames. For frames, this study looks closely at language used by these actors, analysing them for arguments of causality and significance. For arenas, the study looks at where the contest of frames predominantly takes place, in the mass media or through official inquiries. This is analysed by registration of occurrences in both. For factors, the study makes a temporal and situational analysis, based on (political) time and the relevant government sectors the crisis hits. For impacts, the situation of the spheres policy, political and institutional before the crisis are compared with the situation after the crisis.

The sources used in the empirical analysis are categorized in two: primary sources, the main documents in which the exploitation of the crises take place; and secondary sources, that provide either context or another form of valuable information. The Diginotar case has two

expert-based inquiries, one moment of parliamentary inquiry, one document in the media arena, and four conducted interviews as primary sources. The interviews are unique data, the other data is open source. Additionally, it uses 15 secondary documents for its empirical research, including technical evaluations, evaluation reports, policy documents, documents of political communication, journalistic analyses and an academic publication.

Figure 3: overview of all used data

Overview of sources				
	Case 1: Diginotar crisis		Case 2: Snowden revelations	
	Source	Type	Source	Type
Primary sources				
	Onderzoeksraad Voor Veiligheid (2012)	Expert-based inquiry	Kamerhandeling (2014a)	Parliamentary inquiry
	Inspectie Veiligheid en Justitie (2012)	Expert-based inquiry	Kamerhandeling (2014b)	Parliamentary inquiry
	Kamerhandelingen (2011)	Parliamentary inquiry	Respondent A	Interview
	Respondent A	Interview	Respondent B	Interview
	Respondent B	Interview	Respondent C	Interview
	Respondent C	Interview	Respondent D	Interview
	Respondent D	Interview	Nieuwsuur interview (2013)	Conventional media
	NOS press conference (2011)	Conventional media	@brenno (2013a)	Online media
Secondary sources				
	FOX-IT (2013)	Technical evaluation	Kabinetsreactie (2013)	Political communication
	Logica Business Consulting (2012)	Technical evaluation	Kamerbrieven (2013a;b;c;d);(2014);(2015)	Political communication
	Rijksauditdienst (2012)	Evaluation report	Kamervragen (2013b; c); (2014); (2015)	Political communication
	Kamerbrieven (2011a; b); (2012)	Political communication	CSBN 3 (2013)	Policy document
	Kamervragen (2011a; b); (2012); (2013a)	Political communication	CSBN 4 (2014)	Policy document
	NCSS 1 (2011)	Policy document	NCSS 2 (2013)	Policy document
	CSBN 1 (2011)	Policy document	Inkster (2014)	Academic publication
	NRC Handelsblad (2011); (2013)	Journalistic analysis	Johnson et al. (2014)	Academic publication
	Proschinger (2012)	Academic publication	Wright and Kreissl (2013)	Academic publication
			NRC Handelsblad (2014a; b; c); (2017)	Journalistic analysis

The Snowden revelations case has two moments of parliamentary inquiry, four conducted interviews, one conventional media, and one online media document as primary sources. Additionally, it uses 21 secondary documents for its empirical research, including policy documents, documents of political communication, journalistic analyses and academic publications.

3.4 Reliability and validity

There are multiple scientific limitations and considerations to the proposed research design that should be mentioned. These have their implications for the reliability, the degree to which an assessment tool produces stable and consistent results, and validity, the degree to which the research measures what it aims to measure, of the research. Roughly, their origins can be attributed to the characteristics of the cyber domain, the methods of data collection, and limitations that are inherent to the case study design.

In reverse order, the method of case studies inevitably has inherent scientific limitations. In fact, the value of case study methods is debated upon within the scientific community. This manifests in the broader discussion on qualitative vs. quantitative research, which Creswell describes in Part II of his book on methods (2013: 95). The argument is often made that, because of the autotomized methods that are regularly used in quantitative research, the results are often more robust in comparison with qualitative research methods, which often relies on the interpretation of a researcher and the meaning that he or she gives to the findings. According to Gerring (2007), the appropriateness of a research method depends on the purpose of the research. He argues that case study designs have disadvantages against, but also advantages over, quantitative, cross case analyse (ibid.: 37). He argues that the latter is best suited for testing hypothesis across a set of cases, whereas the in-depth analysis methods of the first, provide the insight into the causal processes within cases, thus making it more suitable for generating hypotheses (ibid.). Additional research goals that the case study model is better suited for, include a high internal validity, which is useful when there is a complex causal process, or when the research aims for a deep scope, rather than a broad scope (ibid.). As the optional research design is determined by the unit analysis and/or the unit of observation, the choice is not always up to the researcher. Some variables simply are not quantifiable, or hardly ever observed, making them unsuitable for the large-N, cross-case analyses that quantitative research usually encompasses. This holds true for the units of observation and analysis in this research, which deals with a very concentrated availability of data, and the heterogeneous research population of cyber crises.

Other considerations relate to the characteristics of cyberspace. It is noted that when this domain is researched, two factors can cause complications: the incipiency and the technical character of the domain (Kello, 2013: 37-40). Apparently, the technical complexity of the field is still regarded as a barrier to non-technical studies, for example originating from international relations or governance studies. In this study, it is argued that this consideration is redundant.

The technical character of the domain can be understood on an abstract level, and this is sufficient to theorize the implications this has on other domains, as long as the assumptions are academically informed. This is for example also done in mutual assured deterrence theory in the international relations discussion on nuclear weapons. Technical insight in the way that nuclear weapons work is not required to theorize its implications, just the point of departure that they are lethal. In addition, the incipiency of the domain could have implications for the future relevancy of the results of the thesis and should therefore be considered. This thesis does that in paragraph 2.2.2.

Additionally, scholars have had considerations with acquiring data through interviewing those that are closely involved. As is argued throughout this research, a crisis indicates a situation of contesting interests. Interviewing stakeholders that participated in these contests might be the only way to access certain information, but it runs the risks of a bias. The interviewees might for example engage in 'blame avoidance' in the aftermath of a crisis (Brandstrom and Kuipers 2003; Bovens and 't Hart 1996). Also, the "existing loyalties to third parties very often motivate a tendency to sell a particular story" (Hansel, 2016: 11). On top of that, there is a cognitive discussion on the reliability of the human memory in recalling past feelings and events, even without a manipulative intention (ibid.). These three might cause a bias in the research results, which should be considered in the analysis. This research specifically does that through selecting respondents that have worked in different organizational layers, from decision-maker to operative, verifying the resulting data across the conducted interviews in the next chapter.

4.Empirical analysis

After an elaboration on the background of the case, in which the case is substantiated to the definition of a crisis, the empirical results will be presented in a standardized format. Firstly, the findings from the empirical evidence acquired through interviews will be discussed. Consecutively, the results found in the open source data, consisting of policy documents, evaluation reports, parliamentary inquiries, academic contributions, and journalistic items, are presented.

After this is done on all the research themes (actors, frames, arenas, factors, and impacts), on both cases, this chapter will conclude with a case comparison that serves as an overview of the narrow research findings, which is assisted by visual representation of the found data. This specific format is chosen to present the results of the research in a way that is as objective and retraceable as possible.

4.1 The Diginotar Hack

4.1.1 Background and case substantiation

The Diginotar hack concerns the hack of the former technology company 'Diginotar'. One of the businesses of this company was the issuing of Public Key Infrastructure (PKI) certificates. These certificates are a vital component in the digital infrastructure, because they act as a 'passport' that identifies a digital address. This is done in the following way.

The exchange of electronic data is secured through encryption, to keep the data that is communicated private. One of the regular ways in which this is done is through asymmetric encryption, which uses two 'keys' to encrypt and decrypt data. These keys correspond, meaning that both are needed to decode the respective data. One of these keys is public, and accessible for anyone to encrypt a particular message, but only the one holding the private key is able to decrypt this data. When for example a governmental entity offers its public code, users assume that only this governmental entity gets the information that is being send. In doing so, the user has to trust that the public key is in fact linked with the right private key, owned by this government entity. To build in a check for this process, digital certificates were created. These are issued by companies, and guarantee the reliability of the public keys. Thus, a user can trust the key if it is certified. The certificates issued by Diginotar were used in vital government services, such as the digital identification service DigID, amongst other applications. The system of Diginotar that was issuing these certificates was hacked in the summer of 2011.

The hack surfaced on the 27th August 2011, when an Iranian internet user received an invalid certificate warning from his browser. The certificate was generated on the 10th July 2011 and it quickly became clear that the compromised certificate was issued by DigiNotar, which was successfully broken in to by a hacker. The hacker used his acquired access to the Diginotar systems to sign 'rogue' certificates, allowing him or her (identity is still officially unknown) to listen in on, and possibly modify, the communications of users of services such as Google Gmail, that made use of these compromised certificates, predominantly in Iran. For Google services alone, the estimate is that at least 300,000 distinct users were confronted with, and possibly influenced by, fraudulently issued certificates. The company itself was already aware of this breach, but decided to keep it a secret from the general public and public authorities (GCCS, 2015: 8). Although it compromised the public interest, there was no explicit legal provision prohibiting this before the crisis that followed, which appears to be changed after the Diginotar crisis, which is further discussed in paragraph 4.1.6. The breach implied that trust could no longer be placed in the confidentiality or integrity of data or communications which had been secured with a DigiNotar certificate, which had major potential impact. After this became apparent, several events quickly developed.

On the 29th of August, GovCERT, the national computer emergency response team of the Netherlands, was notified of the attack by CERT-BUND, their German equivalent. DigiNotar itself immediately admits to having been hacked. On September, the 3rd, Dutch government officially announces DigiNotar as an untrustworthy certificate provider, and activated its crisis structures (GCCS, 2015: 9).

Although from that point the Government of the Netherlands treated the Diginotar hack as a crisis, the case must be substantiated in accordance with the theoretical definition of crises outlined in chapter 2.1.1. Recalling this theory, the three critical conditions need to be present to be considered a crisis: a (1) threat, that is (2) urgent, and brings along (3) uncertainty, that threatens the basic structures or the fundamental values and norms of a system and thus necessitate critical decision making, (Rosenthal, Boin, & Comfort, 2001; Boin et al. 2009: 83-84). Furthermore, following the definition drafted in chapter 2.2.2, the situation needs to either take place in cyberspace (type I), or needs to be facilitated through cyber means (type II), to be considered a cyber crisis.

Starting with the fundamental values and norms of a system that are being threatened, in the Diginotar crisis these consists of the assumption that the system of digital certificates, and thus all general forms of digital communication that have become a part of the critical infrastructure, is trustworthy. The Public Key Infrastructure of the Dutch Government

(PKIoverheid), essential in digital services such as the tax return systems, relied on certificates issued by Diginotar. Due to the hack, the fundamental norm of trustworthy digital communication was compromised. This was a *threat* to the functioning of government and government services, as confirmed in several parliamentary hearings (Kamerbrieven, 2011a; b; 2012) and is additionally being underscored in evaluation reports (Fox IT, 2012: 3).

There was a clear presence of *uncertainty* during the developments of the crisis. First of all, through the way in which the crisis should be solved: there was only very limited knowledge about where DigiNotar certificates were being used (GCCS, 2015: 10). Secondly, it was also unclear what the impact would be of revoking DigiNotar certificates: it was noted that abruptly revoking DigiNotar certificates could lead to a 'government blackout' (NRC Handelsblad, 2011).

To prevent such a blackout, there additionally was a strict *urgency* in terms of time pressure. First, the scope of access to communication with government, and private, services was unknown. The worst possible scenario would be that all the data exchanged using Diginotar certificates was in the hands of the attacker, and thus compromised. Secondly, the company Microsoft decided to revoke all support for Diginotar certificates within ten days of the 6th of September, giving the government service an extremely short time to replace them (GCCS: 9).

With cyberspace being the different layers of the realm of computers, the Public Key Infrastructure and the system of digital certificates that was abused in the Diginator hack is a part of the logical layer of considerations and decisions (Clark, 2010: 1-4). Additionally, the access to data was compromised, which situates the crisis additionally in the layer of information and data (ibid.). The Diginotar crisis therefore is a clear case of a type I crisis occurring *in* cyberspace. In addition, the crisis conditions constituted a specific question in the interviews conducted for this research.[15] All respondents considered the Diginotar hack a crisis containing the components threat, urgency and uncertainty. Concluding, multiple sources indicate presence of the theoretical crisis conditions in the Diginotar crisis. It can therefore be considered a crisis suitable for the theoretical model of crisis exploitation.

4.1.2 Actor analysis

This paragraph seeks to find the answer to the subquestion *which actors are contending in the aftermath of the respective crisis?* Recalling the theory on actors, they are the individuals or

[15] See Appendices B & C.

organizations that participate in the contest of frames in the relevant arenas that ensue in the aftermath of the respective crisis, and are indicated by the crisis-type rhetoric used. Furthermore, actors are found in two spheres, corresponding with the impacts of crises: the (1) political sphere, concerned with the alteration of levels of political support, and consisting of incumbent actors holding public office, and critic actors criticising public office-holders, and (2) the policy/institutional sphere, concerned with keeping or changing the pre-crisis policy, consisting of status-quo players, concerned with protecting policy from change, and change advocates, concerned with changing policy. To answer the subquestion question, this paragraph will provide an overview of all the actors that have employed crisis type rhetoric in the arenas outlined in 4.1.4, on more than one occasion. Within the data acquired through open sources, the following actors were found to be actively and purposefully participating in the both spheres.[16] Additionally, it is indicated if an actor is mentioned in the one or more of the conducted interviews. An overview of the respective actors can be found in figure 4.

Incumbent actors

The incumbent actors were the actors that were formally responsible at the time and occurrence of the Diginotar crisis. Constitutionally, the political responsibility lies with the heads of the departments of the governmental sectors, and by ultimate extension, with the prime minster of the Netherlands. No evidence indicates that the Diginotar crisis is ever scaled to this political level, leaving prime minister at the time, Mark Rutte, out of the picture. Rather, the heads of the two main departments governing the cyber domain, the Ministry of Security and Justice, and the Ministry of Interior, were called upon their responsibility in both the media and official inquiry arena's. The ministry of Security of Justice was headed by minister Ivo Opstelten, whereas the Ministry of Interior was headed by Piet Hein Donner. Both actively engaged in the contest of frames in the aftermath of the crisis. In the parliamentary arena, both had an equal role, whereas in the media arena, Piet Hein Donner acted as the prime focal point (NOS, 2011). Furthermore, evidence of his active role is found in the multiple instances, for example in Kamerhandelingen (2011: 54:23); and Kamerbrief (2012). In the interview sources, respondents unanimously agreed upon this depiction of his role (Interview A; B; C; D).

[16] Although there is a theoretical notice that actors should be regarded multi-dimensionally, meaning that they can be either actor in both spheres, the actors found in this case align in both spheres, and are therefore combined in the overview.

Subsequently, the same is true for Ivo Opstelten. Examples of his role found in open sources are Kamerhandelingen (2011: 2:17:17), and Kamerbrief, (2011c).

Critic Actors

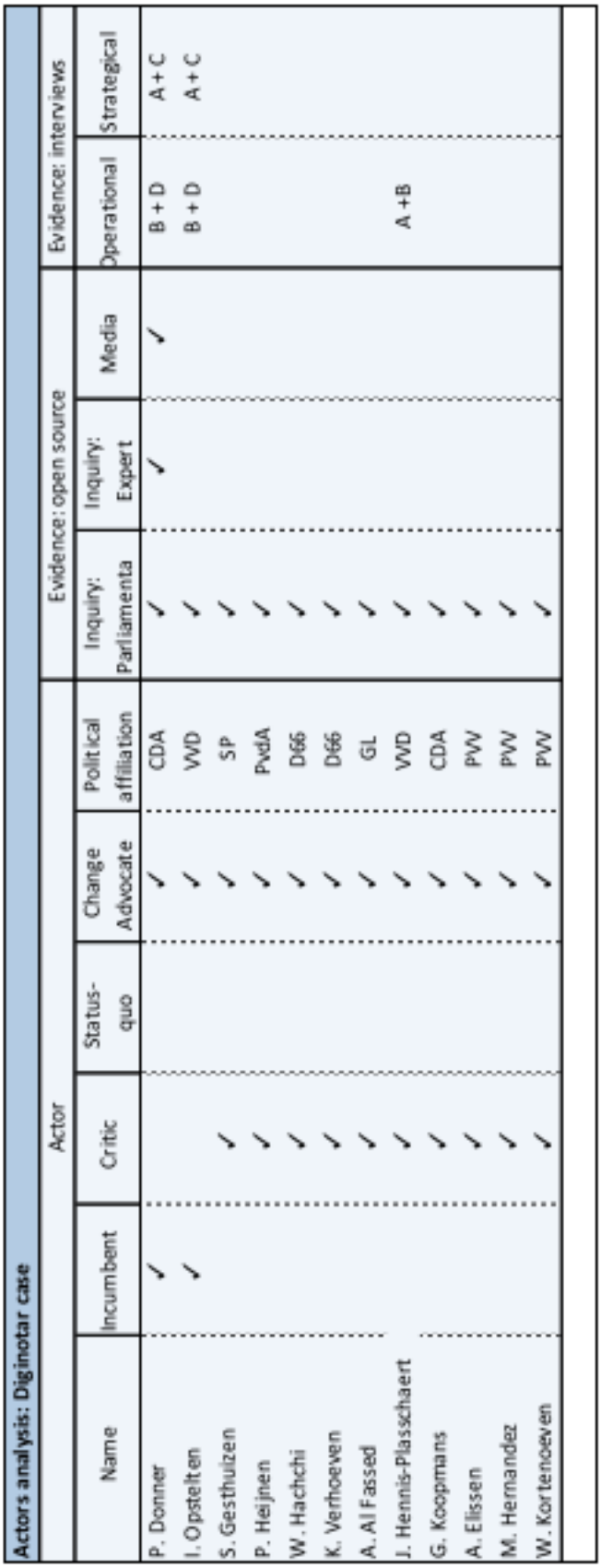
The critics actors are mostly found in the parliamentary inquiry following the crisis. These actors are either oppositional, or coalitional members of parliament, depending on political affiliation. This includes the following ten actors: Ms. Gesthuizen, as a member of Parliament for SP (Kamerhandelingen, 2011: 0:22); (Kamervragen. 2011e). Mr. Heijnen, as a member of Parliament for PvdA (Kamerhandelingen, 2011: 6:23); (Kamervragen. 2011e). Ms. Hachchi, as a member of Parliament for D66 (Kamerhandelingen, 2011: 15:43); (Kamerbrief 2011c). Mr. Verhoeven, as a member of Parliament for D66 (Kamervragen, 2011d); (Kamerbrief 2011c). Mr. El Fassed, as a member of Parliament for GL (Kamerhandelingen, 2011: 20:17); (Kamervragen, 2011c). Ms. Hennis-Plasschaert, as a member of Parliament for VVD (Kamerhandelingen, 2011: 20:17); (Kamervragen, 2011c); mentioned in interview A and B. Mr. Koopmans, as a member of Parliament for CDA (Kamerhandelingen, 2011: 33:40); (Kamerstuk, 2012). Mr. Elissen, as a member of Parliament for PVV (Kamerhandelingen, 2011: 45:51); (Kamervragen, 2011a). Mr. Hernandez, as a member of Parliament for PVV (Kamervragen 2011a); (Kamervragen, 2011b). Finally, Mr. Kortenoeven, member of Parliament for PVV (Kamervragen 2011a); (Kamervragen, 2011b).

Non-public actor

As found in the previous chapter 2, there is reason to believe that due to the characteristics of the cyber domain, non-public actors, such as civilians and private, can have a strong influence in the crisis exploitation process. Although there is no evidence found of non-public actors directly contending in the contest of frames, as acted out in the arenas of mass media and official inquiry, there is evidence suggesting that some private actors had significant influence through the incumbent actors nonetheless. Notably, through the institutions ‘ICT Response Board’ (IRB), and the ‘Cyber Security Raad’ (CSR), that both consist of at least 50% actors from the private sector. Both institutions have been consulted during the crisis and in its aftermath (IVJ, 2012: 20-21). The exact consistency of the Incident Response Board is non-disclosed and flexible (IVJ, 2012: 20). The members of the Cyber Security Council are disclosed, and include representatives of KPN Telecom, CGI, PostNL, ECP, Schiphol Group, and TenneT (NCSS, 2011: 5). Formally, both have an advisory role. Both open sources and the interviews (A-D) however confirm the influence that both actors have had in the aftermath of

the Diginotar crisis on the position of the incumbent actors. In the first press conference after the Diginotar crisis, minister Piet Hein Donner of the Ministry of Interior acknowledged the role that the CSR would play in the policy change that might follow the crisis (NOS, 2011: 13:11).

Figure 4: overview of actors in the Diginotar crisis



Actors analysis: Diginotar case												
	Actor						Evidence: open source				Evidence: interviews	
Name	Incumbent	Critic	Status-quo	Change Advocate	Political affiliation	Inquiry: Parliamenta	Inquiry: Expert	Media	Operational	Strategical
P. Donner	✓			✓	CDA	✓	✓	✓	B + D	A + C
I. Opstelten	✓			✓	VVD	✓			B + D	A + C
S. Gesthuizen		✓		✓	SP	✓				
P. Heijnen		✓		✓	PvdA	✓				
W. Hachchi		✓		✓	D66	✓				
K. Verhoeven		✓		✓	D66	✓				
A. Al Fassed		✓		✓	GL	✓				
J. Hennis-Plasschaert		✓		✓	VVD	✓			A +B	
G. Koopmans		✓		✓	CDA	✓				
A. Elissen		✓		✓	PVV	✓				
M. Hernandez		✓		✓	PVV	✓				
W. Kortenoeven		✓		✓	PVV	✓				

4.1.3 Crisis rhetoric and contest of framing

This paragraph analyses the frames that the respective actors tried to push in the aftermath of the crisis, determining which frame became the dominant view, and through which crisis rhetoric. This is linked to the subquestion: *what type of frame are the contending actors trying to push?*

First, it must be noted that there is a somewhat deviant situation in the Diginotar crisis. As further discussed in 4.1.5 (situational/temporal factors) and 4.1.6 (impacts), the Diginotar had a peculiar timing, for it occurred during some of the most rigorous reforms in the Dutch cyber policy, invoked by the newly formed Rutte I Administration (2010-2012) (Interview A, 13:42). In accordance with the first National Cyber Security Strategy (NCSS 1, 2011) drafted in February 2011, an entire new policy directive was being set up – Directie Cyber Security (DCS) – that included the newly formed operative unit 'Nationale Cyber Security Center' (NCSC), in which GOVCERT, the predecessor of the NCSC, would absolve. Additionally, efforts of creating an advisory council, the 'Cyber Security Raad' (CSR), were aimed at including the private sector in decision making. The 'ICT Response Board' (IRB), aimed at including the private sector in crisis management, had just been concluded in June 2011. On top of that, the Diginotar crisis occurred in the middle of an institutional transition. In fact, due to the institutional merger of the policy fields of justice and security in the newly formed Ministry of Security and Justice, the policy domain of cyber, and its main entity GOVCERT, the national computer emergency response team (CERT), was being transferred from the Ministry of Interior and generally transformed. This has consequences to what is regarded as the status quo in the framing contest within crisis exploitation. Usually, the status quo is a situation that has remained the same for a long period of time, and is challenged by a crisis. In the instance of the Diginotar crisis, the status quo situation was, reversibly, a situation that was characterized by policy, political, and even institutional change.

With the actors in mind, it is now necessary to look at the frames that they tried to push, and which frame type acquired dominance. Recalling from the theoretical framework, there are three types of frames, two of which are considered possible frames in this model: type II, and type III. To indicate crisis exploitation, the used crisis type rhetoric is analysed. More specifically, the clash over two different characteristics of the crisis is analysed: its significance, and its causality, in which the blame of the crisis is being framed as an incident, or a symptom of something wrong.

Significance

The clash over significance is characterized by the debate whether the crisis was an incident or a symptom of there something being wrong. Actors either minimize, acknowledge, or maximize the significance of the event. Data originating from the conducted interviews suggests the following: the Diginotar crisis was unanimously perceived as a symptom of the vulnerabilities in the public management of the cyber domain, both by incumbent and critic actors. In the open source data, the significance of the crisis was acknowledged by all actors from eruption to end. Sometimes, this occurred literally, when in the parliamentary inquiry critic actor El Fassed noted:

> "The Diginotar debacle, as bad as it looks like, is a symptom of a chronically ill relation of the government and the ICT sector, as well as the deficient interest the government has in the security of ICT and our general privacy." (Kamerhandeling, 2011: 3)

The previous quote additionally is an example of the attempts made to maximize the crisis by oppositional actors, also exemplified by Gesthuizen calling the crisis "digital doom" (ibid.: 1); and Heijnen whom claimed that "the government would have gone bankrupt, were it a bank" (ibid. 2011: 4). An observation is that the above trend crosses political dividing lines, with member of incumbent party VVD Plasschaert stated maximized the significance of the crisis is "a threat to human lives" (ibid.: 5) and "as leak as a basket" (ibid.: 4).

Causality

The clash over causality is characterized by actors who blame the crisis on either endogenous or exogenous factors. In the interview data, there is a broad consensus that within the government, the notion was present that the digital infrastructure was quite vulnerable, one respondent stating that "it was not the question if, but rather when a crisis like this would happen" (Interview D). This translates into the crisis having endogenous causes, originating from a fragile balance between ICT and security within the government.

Most of the findings in the interviews are confirmed in the open source data, however it additionally indicates a more critical interpretation of the crisis, differing along the spectrum of actors. A plethora of attempts are made to endogenize the causes of the crisis by oppositional actors (Kamerhandelingen, 2011), and some form of endogenization is also found with incumbent actors. For example, minister Donner notices the following in his press conference:

> "Personaly, I see an urgent cause to look at the future, and look at legal obligations to report vulnerabilities to government entities, if they have the potential to compromise

> the public interest […] and a need for additional warranties in the current certificate authorisation system" (NOS, 2011b: 15:41-16:35).

This quote is an indication of the belief incumbent actors had that the digital breach at Diginotar compromised the Public Key Infrastructure certificate system of the government, which itself was vulnerable: an endogenous cause. This applies to both the incumbent actors Donner (Kamerhandelingen 2011: 9-10) and Opstelten (Kamerhandelingen, 2011: 19).

Nevertheless, both expert-based inquiries confirm that the breach was at the responsibility of the company Diginotar, and that the government crisis management structures and technical operations had acted well upon this, considering the incipiency of the domain and urgency of the crisis (Onderzoeksraad Voor Veiligheid 2012: 82; Inspectie Veiligheid en Justitie, 2012: 8-9).

Frames

The clash in causality and significance clearly reflects in types of frames that were used in the aftermath of the Diginotar crisis. Type II frames, predisposing the critical threat of the crisis to defend those policies and agents responsible for the status quo, were frequently seen by the incumbent actors and status quo players. Type III frames are frequently pushed by the critics and change advocates, arguing that the crisis predisposes a critical opportunity to change the current policies and/or those in office are being held responsible, and the argument is made that they should be reformed substantively or replaced in their entirety.

In the interviews, the respondents interpreted the crises as a critical opportunity type III frame (interview B), or as a combination of the elements of type II and a type III frames, meaning that the status quo of the initiated changes was under critical threat, and that this crisis could provide additional salience to these changes (Interview A: 12:10; Interview C: 2; Interview D: 2). As mentioned, it is observed that in the identification of frames, all actors seem to opt for changes within the cyber and ICT governmental sector, that were in fact already initiated before the occurrence of the Diginotar crisis. With the 'status quo' as a state of policy, political, and even institutional change, the contest of frames had a focus on their extent and speed. Therefore, the common frame that can be deduced from the crisis-type rhetoric applied in the aftermath of the Diginotar crisis is a type II frame, with the paradox that all actors are advocates of change, change being the status quo.

4.1.4 Exploitation arenas (media and inquiries)

This paragraph analyses the arena's in which the crisis exploitation predominantly took place. It answers the subquestion: *in which arenas was the exploitation of the crisis principally acted out?*

The two arenas recognized in the theoretical framework, mass media and official inquiry, are both analysed for the occurrence of actors employing crisis type rhetoric. Open source data suggest that little of the contest of frames occurred in the media arena, consisting of television, newspapers, and online. Most items found are of a descriptive nature, rather than a substantive employment of crisis type rhetoric as specified in the definition of framing. There are two exceptions to this: both the press conferences held by Piet Hein Donner, the head of the Ministry of Interior. Respectively, these occurred on the 3rd of September (NOS, 2011a) and 6th of September 2011 (NOS, 2011b). In both instances, Donner reflects on the nature of the crisis, and speculates to the consequences these should have.

These findings are in line with the information found in the interviews. Three of four notice that items in media were of little significance in the aftermath of the crisis (Interview A, B, D), with respondent c stating that on a communication level, the crisis was insignificant due to a lack of media interest.

The opposite is true for the arena of official inquiry. In the open sources both forms of official inquiry, parliamentary and expert, are observed. Expert inquiry had two separate committees considering the crisis and its aftermath, one being the oversight institute for the Ministry of Security and Justice (Inspectie Veiligheid en Justitie, 2012), and the second being of an independent nature, through an evaluation institute (Onderzoeksraad Voor Veiligheid, 2012). Alongside the expert based forms of inquiry, the Diginotar crisis case also saw multiple moments of political inquiry through parliament. Most significantly, the central parliamentary debate on the 13th of October (Kamerhandeling, 2011). Additionally, other moments of parliamentary inquiries include Kamerbrief (2011a; b; c); Kamerbrief (2012); Kamervragen (2011a; b; c; d; e) Kamervragen (2012) and Kamervragen (2013a). This information is in accordance with the information provided by the respondents in the interviews.

4.1.5 Actor propensities as a result of situational and temporal factors

This paragraph discusses situational and temporal factors, and the actor propensities they have caused in the respective crisis. In doing this, it answers the question: *what situational and temporal factors shaped the actor propensities?*

In the theoretic framework, it became apparent that some situational and temporal factors are of influence in shaping the actor propensities. Temporal factors concern the situation of the crisis in political time, i.e. the respective time until the next election and the time of political incumbency. In the multi-party electoral democracy of the Netherlands, cabinets serve for four consecutive years. On June, the 14th of 2010, a parliamentary election was held and after 127 days of negotiation, on the 14th of October, the cabinet Rutte I was formed, consisting of the political parties VVD and CDA. This cabinet had a minority in both houses of the Netherlands and thus required the support of a third party, the PVV, which it got through an agreement of toleration, wherein the PVV traded parliamentary support for influence in the policy direction of the cabinet. Diginotar happened eight months after this, so elections were 40 months away, and thus quite irrelevant at the time. Additionally, the period of incumbency for Donner on the governmental level was a total of 96 months in office, divided over three terms.

The situational factors concern the scope of the crisis, and the governmental issues it spanned. Although it did span the digital infrastructure, recognized as a critical infrastructure, the Diginotar crisis spanned few other governmental issues. In the beginning, the Ministry of Finance, represented by undersecretary Frans Weekers, joined the crisis structure, but this department quickly disappeared from the public responsibility structure in the aftermath of the crisis. Public responsibility remained with the Ministries of Security and Justice, and Interior, respectively headed by ministers Opstelten and Donner. Additionally, the crisis was never scaled to the highest level of public responsibility, Prime-Minister Rutte. Thus, it can be concluded that in comparison to the broad- and deepness of the cases studied in Boin et al., the scope of the crisis was narrow and shallow, (2009; see: ‘t Hart, 2009).

Beyond the factors outlined in Boin et al. there might be a different situational factor influencing the actor propensities in the Diginotar crisis. Due to the incipiency of the cyber domain, the Diginotar crisis occurred in a period of institutional transition, which may have had a large influence on the propensities of actors. Rather than acting with a clearly established status quo, as relevant in all the domains studied in Boin et al. (2009), contenders in the Diginotar hack had to contest a status quo that is characterized as being volatile *itself*. During the crisis, the cyber domain was already undergoing drastic changes, and at no point the Diginotar hack has been blamed on the elite, as seen in the next paragraph. In other words, the dominant view is that the ongoing changes, nor the incumbents responsible for them, were not a cause the crisis, but rather a situational, or perhaps additional, factor at play.

In sum, the Diginotar crisis is characterized by a long period of incumbency, long period to the next election, a narrow and shallow scope, where additionally, the incipiency of the domain may have been another factor that has influenced the actor propensities.

4.1.6 Policy, political and institutional impacts

This paragraph analyses the policy, political and institutional situation before the crisis, and compares it with the respective situations after the crisis. It answers the subquestion: *what impacts of the crisis are observable?* It is important to answer the question as a theory of crisis exploitation needs to capture how the clash between frames produces particular types of political and policy consequences. Following this logic, it is important to look at what has changed after a crisis, in relation to the situation before the respective crisis. Recalling the three spheres – policy, political and institutional – the situation before the crisis will be discussed for all three.

In terms of policy, the cyber domain was in the process of expansion, as part of the electoral program of the newly installed cabinet. A first national strategy was launched in February 2011, which included plans for a more "extensive and comprehensive policy approach" (NCSS, 2011: 3). In this approach, a strong focus was put on developing public-private-partnerships. In the political sphere, the cyber domain was in the process of transferring the responsibility of the public cyber domain from the minister of interior to the minister of security and justice. This institutional transition is also the main characteristic of the respective institutional sphere, preceding the Diginotar Hack.

In terms of policy, evidence suggesting that Diginotar influenced its direction is found in both open sources and the interviews. Specifically, in two ways: a 'meldplicht', the report duty - legal obligation to report vulnerabilities that might cause national havoc - and the inclusion of an additional warranty in the Public Key Infrastructure of the government of the Netherlands. Where the latter is a technical, instrumental adjustment in implementation practices, the former is much more than that.

The 'meldplicht' was introduced by Mw. Hennis-Plasschaert in the parliamentary arena in the aftermath of the Diginotar crisis. It proposed a legal obligation to notify a central authority of any significant data leaks or break- ins within an organisation, arguing that in the case of DigiNotar, this would have led to an earlier awareness and understanding of the extent of the problems, and would have prevented it from becoming a crisis (GCCS, 2015; Kamervragen, 2011e). It came into effect on the 1st of January 2016. This motion changes the concept of responsibility in the cyber domain, and gives it the means to enforce this

responsibility, which is a change to the fundamental values in this policy domain. The policy situation has thus seen technical, instrumental adjustments in regulation and implementation practices, 'secondary' policy change, but also a more fundamental, 'core' policy change.

In the political sphere, no evidence is found of an alteration in political support for the incumbent leaders, neither in the interviews nor in the open source data. In the categorization of the theoretical framework, no evidence was found of elite damage, occurring when the blame of a crisis is successfully focussed to the officeholder. Rather it appears that in the aftermath of the Diginotar crisis either elite escape, when blame is diffused or displaced, or elite rejuvenation, meaning that instead of blame there is support and praise for the officeholders, took place. Both the incumbents Opstelten and Donner were subject to some form of criticism during the parliamentary inquiry (Kamerhandeling, 2011). Evaluations within the expert inquiries show more evidence of appraisal. One of both has the main conclusion that the crisis was managed very well (IVJ, 2012: 5). This is appraisal is echoed in one of the interviews, stating that "Donner and Opstelten are two of the four reasons why the Diginotar had a good ending" (interview D: 32:52). It should additionally be noted that no evidence was found that the Diginotar crisis in any way influenced the politics on a higher level, concerning the prime-minister Mark Rutte, in the political situation that unfolded 8 months after the Diginotar crisis, which caused a coalition break and new elections.

Somewhat unconventional are the institutional effects of the Diginotar crisis. As the crisis occurred in the middle of an institutional transition, it is hard to measure the specific role of the crisis. With certainty however, the crisis did not question the entire institutional integrity of a cyber policy sector, therefore, the crisis cannot be regarded as an institutional crisis. However, there is evidence of a dispersion in the institutional field. As mentioned, the institutional field is characterized by a transition from the Ministry of Interior to the Ministry of Security and Justice, including the governing entity GovCERT responsible for handling the Diginotar crisis. During the crisis, this entity was still formally attached to the Ministry of Interior, as it had been since its founding year. The above situation made the question of responsibility difficult. In handling the crisis, the Ministry of Interior became the main focal point in terms of responsibility, but the Ministry of Security and Justice remained closely involved. In practice, the institutional demarcation was clear: subjects concerning the crisis itself were handled by the Ministry of Interior, whereas subjects of a consequential matter were handled by the Ministry of Security and Justice (Kamerhandelingen, 2011: 54:32; 2:17:17). In terms of the institutional transition, anecdotal evidence that the Diginotar crisis had a catalysing role is found in the interviews, with respondents stating that the salience the Diginotar crisis

gave to the field of cyber security, in addition to the newly found institutions, determined a large growth in resources and significance of these institutions (Interview A; C; D). One of the respondents described a specific change in the position of critic actor Hennis-Plasschaert. In a general parliamentary meeting, she allegedly called the newly presented National Cyber Security Strategy an 'exaggeration', but came back from this position in the aftermath of the Diginotar crisis (Interview D: 29:35). This can however not be verified in open sources.

4.1.7 Subconclusion Diginotar Hack

In summary, twelve actors were identified that purposefully employed crisis type rhetoric to influence the consequences of the Diginotar crisis. In the contest of frames that occurred in the aftermath, a type II frame was observed as the dominant frame, with the paradox of 'change' as the status quo, in which the crisis' significance was acknowledged by some and maximized by other actors. Additionally, the crisis was predominantly interpreted as a symptom, with most of its blame attributed to exogenous causes concerning the negligence of the Diginotar company, that kept the breach a secret, but endogenous factors are identified in the insufficient legal framework allowing this to happen, and the lack of warranties in the digital certificate system used by the government, that proved that it could not guarantee reliable government services and communication. In terms of arenas, it was furthermore observed that there was relatively little media attention for the Diginotar crisis, as well as multiple official inquires, both parliamentary and expert based. In the situational factors, it was observed that the crisis was situated far away from an election, concerned long periods of incumbency, and was both narrow and shallow in scope, covering the second highest level of public responsibility and two real policy sectors. In addition, a side note was made to the situational factor of the institutional transition the cyber domain was undergoing when the crisis developed. In terms of impact, evidence was found for a connection between Diginotar and the core policy changes that were invoked in its aftermath, notably the 'meldplicht', the report duty, and changes in the certificate system. Although the Rutte I cabinet lost its majority not long after the Diginotar crisis, no evidence for a connection between the two events is found. In terms of political support for the relevant incumbents, no notable alterations are observed. Finally, the institutional reforms that occurred in the aftermath of the Diginotar crisis were initiated (just) before the crisis developed and can therefore not be contributed to this particular crisis. However, some evidence suggests that the process of institutional change was catalysed by the Diginotar crisis, which is explained by the increase in salience that the policy domain acquired as a result of the crisis.

4.2 The Snowden Revelations

4.2.1 Background and case substantiation

With ‘The Snowden Revelations’, this thesis refers to the situation that occurred after the biggest leak of confidential intelligence data in history. In this incident, whistle-blower Edward Snowden leaked an estimated amount of 1.7 million highly classified files belonging to the United States of America’s National Security Agency (NSA) to investigative international media, including media outlets the Washington Post, The Guardian, and Der Spiegel.

The data leak exposed the extent of the global surveillance program of the United States of America, which outraged many of its allied countries. Snowden claimed that the NSA had access to, and collected, data of millions of people. He had acquired the proof, the classified files, as a private contractor for the NSA, through security company Booz Allen Hamilton. In June 2013, the first of these files were published simultaneously by The Washington Post and The Guardian, instantly causing havoc among the globe. Roughly three factors caused outrage: the extent to which developed technologies such as the PRISM program could collect data, the scale on which this was happening, and the international exchange of this data between intelligence services (Inkster, 2014).

The havoc varied between countries. For example, in Germany, the outrage was mostly focussed on files that were released that proofed the tapping of the communication of the German Bundeskanzlerin Angela Merkel, causing a diplomatic conflict between both countries. In the Netherlands, an internal crisis situation developed in the second half of 2013, which had a climax in February 2014.

The start of this was a publication on the 5th of August 2013, in German magazine Der Spiegel, one of the outlets Snowden had trusted with publishing the files (Gude, Poitras & Rosenbach, 2013). In the article, with the subject ‘transfers of mass data from Germany to aid the US Surveillance’, it was mentioned that the intelligence service of the Netherlands had transmitted over 1,8 million meta-data files to its U.S. counterpart in the period 10-12-2012 to 10-01-2013. From this information, it was claimed that the Netherlands had extensive contracts with the NSA, in which huge piles of meta data were send. Metadata can be understood and described as ‘data about data’, for example the frequency, duration, and direction of the telecommunication in the Netherlands. This data is used in big data analyses, aiming to reveal patterns valuable for the intelligence community, which can for in its turn serve as evidence in court.

After context to the number 1,8 million was given through a journalistic report in the NRC Handelsblad, pressure to account for this was put on the Dutch government (2013). This pressure accumulated through the parliamentary questions the chain of events provoked (Kamervragen, 2013b; c). Most of this pressure was taken off after the minister that carried political responsibility on the policy of the Dutch intelligence services, Minister of Interior Ronald Plasterk, discussed the topic in journalistic news show *Nieuwsuur* on the 30th of October (2013). During this interview Plasterk stated that the Dutch intelligence services had not collected the 1,8 million files discussed in the Snowden revelations, and consequently, had not provided them to the NSA. Rather, the NSA had collected these files on its own account, without authorization by the Dutch government – an act which he condemned and considered unacceptable (Nieuwsuur, 2013: 2.55). Plasterk repeated this statement in parliament, which effectively focussed blame of the incident on the NSA (Kamerbrief, 2013b; c). This would have likely been the end of the case, if it weren't for internal sources that disputed Plasterks' statements in the NRC Handelsblad (2013). A group of privacy advocates took this as a cue to launch a civil lawsuit against the government, which eventually resulted in a retraction and reiteration of the statements of Plasterk in a letter to parliament on the 4th of February 2014 (Kamerbrief, 2014). In this 6-sentence letter, the ministers of Defence and Interior stated that

> "additional research and analysis […] resulted in the conclusion that the Data was collected by the Sigint services, in reference with combatting terrorism and foreign military operations, and, in accordance with the law, shared with the U.S. intelligence services" (ibid.: 1).

From this point on, a crisis quickly unfolded, resulting in two points of parliamentary inquiry (Kamerhandeling 2014a; b).

The crisis case substantiation should be discussed, since there is some leeway for discussion to the extent of which the situation was in fact a crisis. Considering the components of a crisis as discussed in chapter 2.1.1 and the additional conditions of cyber crises in chapter 2.2.2, it could be argued that this situation is insufficient to be considered a cyber crisis. Recalling, a cyber crisis is a serious threat to the basic structures or the fundamental values and norms of a system, either taking place in cyberspace or facilitated through cyber means, which, under time pressure and highly uncertain circumstances, necessitate making vital decisions. It can be argued that the relatively long timeframe, 5th of August 2013 – 5th of February 2014, indicates a lack of urgency. Following, it can be argued that the real crisis that enveloped can be subscribed to the act of a minister allegedly lying to parliament, a constitutional crime, rather than the cyber surveillance itself. This argument is additionally substantiated by a lack of

upscaling in the crisis structure of the Netherlands, which was a realistic option considering the extent of foreign intelligence involvement in the Dutch society. To the contrary, this thesis argues that the situation *was* a crisis, and it offers two forms of evidence to substantiate this argument.

First, the content analysis of both parliamentary inquiries of the political crisis that enveloped in the aftermath of the crisis situation offers strong evidence that the Snowden revelations invoked a fundamental discussion on the values and norms of the Dutch society. Namely, the discussions on the collection and use of metadata for intelligence services, and, additionally, the extent to which the Dutch intelligence service should cooperate with its American counterpart. This is best indicated by the titles of both parliamentary inquiries: Collection of metadata on mobile traffic by the Dutch security services (Kamerhandeling, 2014a); Eavesdropping by the NSA (Kamerhandeling, 2014b). Although the allegations of misleading parliament by Plasterk, and the consequences to this action, were present, there is evidence found in the content analysis of the discussion on the threat to fundamental societal norms (privacy), threatened by domestic and foreign intelligence agencies.

Secondly, the above argument corresponds with most of the findings in the interviews. All of the four interviewed experts that were given the definition of cyber crises used in this thesis found it applicable to the Snowden Revelations. To this, only respondent C had a slight deviation, arguing that officially, she only regards incidents that are 'scaled up' in the crisis management structures as real crises.

In sum, there was a threat to the fundamental structures of the Netherlands, for it could no longer viably guarantee its citizens' constitutional right to privacy due to interference of domestic and international intelligence services. There was an uncertainty in the extent to which the NSA had interfered in the cyber context of the Netherlands, and what capabilities they had to do this. Furthermore, there was a sense of urgency to respond to the public outrage that had surfaced, especially with the huge amount of attention the situation had gotten in conventional media, and quickly found its way to the political arena. All of this was facilitated through cyber means, leading this thesis to conclude that the Snowden Revelations invoked a type 2 cyber crisis.

4.2.2 Actor analysis

The actors participating in the contest of frames are indicated by their use of crisis type rhetoric in the aftermath of a crisis, as displayed in one of the arenas official inquiry, or media. These actors are further divided in the subgroups incumbent, critic, and non-public. To substantiate

their relevancy, each actor is provided with a reference to the occasion where they displayed crisis-type rhetoric, originating for both open sources and interview sources. An overview of the respective actors can be found in figure 6.

Incumbent actors

The main incumbent actors are the actors that carry the political responsibility of the sector(s) in which the crisis takes place. These sectors are indicated in the specific structure of ministries, with the ultimate political responsibility of these ministries lying with the prime minister of the state, Mark Rutte. Although on some occasions, Rutte was recorded with comments on the Snowden revelations and the crisis it invoked in the Netherlands, the main responsibility was at the account of one political incumbent: the head of the Ministry of Interior, responsible for the intelligence service, Ronald Plasterk. Plasterk actively engaged in interpreting the crisis on several occasions, for example in Kamerhandeling (2014a: 3:45:13), and Kamerhandeling (2014b: 30) in the official inquiry arena, and Nieuwsuur (2013) in the media arena. Furthermore, political responsibility is found in the government sector of the Ministry of Defense, responsible for military intelligence and the collection of the metafiles, headed by minister Jeanine Hennis-Plasschaert. She actively participated in the interpretation of the crisis, for example in Kamerhandeling (2014a: 06:04:38), and Kamerhandeling (2014b: 4:45:45).

Secondary, the sectors of the Ministry of Foreign Affairs and the Ministry of Security and Justice were involved, respectively with the topics of the cooperation with the U.S., and the legal framework of the intelligence service, as seen in Kamerbrief (2013a) and Kamerbrief (2013c).

Critic Actors

The critics actors are mostly found in the parliamentary inquiry following the crisis. These actors are either oppositional, or coalitional members of parliament. This includes the following 22 actors: G. Schouw, as a member of parliament for D66 (Kamerhandeling, 2014a: 2:01; 2014b: 8:41), L. Bontes, as a member of parliament for Groep Bontes (Kamerhandeling, 2014a: 16:09; Kamerhandeling 2014b: 1:19:57), R. Raak, as a member of parliament for SP (Kamerhandeling 2014a: 10:21; Kamerhandeling 2014b: 0:35), B. Ojik, as a member of parliament for GL (Kamerhandeling, 2014a: 19:10), M. Thieme, as a member of parliament for PvdD (Kamerhandeling 2014a: 24:31), M. Bosma as a member of parliament for PVV (Kamerhandeling, 2014a: 29:05; Kamerhandeling 2014b: 1:12:04), M. Toorenburg, as a member of parliament for CDA (Kamerhandeling, 2014a: 35:14; Kamerhandeling 2014b: 1:23:26), J. Recourt, as a member of parliament for PvdA, Kamerhandeling (2014a: 41:55;

Kamerhandeling, 2014b: 1:33:45), K. Dijkhoff, as a member of parliament for VVD (Kamerhandeling, 2014a: 1:40:27; Kamerhandeling 2014b: 26:16), G. Segers, as a member of parliament for CU (Kamerhandeling 2014a: 2:03:59; Kamerhandeling 2014b: 1:07:21), R. Bisschop, as a member of parliament for SGP (Kamerhandeling, 2014a: 2:09:18), N. Klein, as a member of parliament for 50PLUS (Kamerhandeling, 2014a: 2:13:49), A. Pechtold, as a member of parliament for D66 (Kamerhandeling, 2014a: 9:42:19), E. Roemer, as a member of parliament for SP (Kamerhandeling, 2014a: 9:44:53), G. Wilders, as a member of parliament for PVV (Kamerhandeling, 2014a: 09:50:05), S. Buma, as a member of parliament for CDA (Kamerhandeling 2014a: 09:53:04), D. Samsom, as a member of parliament for PvdA (Kamerhandeling, 2014a: 9:55:07), H. Zijlstra, as a member of parliament for VVD, (Kamerhandeling, 2014a: 09:57:43), A. Slob, as a member of parliament for CU (Kamerhandeling, 2014a: 9:59:23), K. Staaij, as a member of parliament for SGP (Kamerhandeling, 2014a: 10:02:42), and finally, L. Voortman, as a member of parliament for D66 (Kamerhandeling, 2014b: 18:22).

Non-public actor

There is reason to believe that due to the characteristics of the cyber domain, non-public, such as civilians and private, actors can have a strong influence in the crisis exploitation process, due to the dispersed actor field within the domain. In the Snowden Revelations case, evidence is found that a non-public actor heavily influenced the developments of the interpretations of the crisis. As introduced, initially, the crisis was successfully framed as exogenous, with Plasterk focusing blame on the NSA in his Nieuwsuur appearance (2013: 2:55). This was however contested in a civil lawsuit against the state, through a 'Wet openbaarheid van bestuur', procedure. A coalition under the name 'Burgers tegen Plasterk' was joined by journalist and hacker Brenno de Winter, who frequently criticized Plasterk and the government through various channels, including conventional (VPRO, 2013) and online media, through twitter (see figure 5), and blogposts (TPO, 2013). Using these outlets, he accused the government in general, and Plasterk in particular, of laundering data. The lawsuit in which he took part led to the rectifications on the 5th of February, that invoked the crisis situation. The pivotal role of De Winter in this is often acknowledged in the political inquiries (fe. Kamerhandelingen, 2014b: 18:23) and the interviews (B+A).

Figure 5: tweet by Brenno de Winter (@brenno, 2013a)

Figure 6: overview of actors in Snowden Revelations crisis

Actors analysis: Snowden Revelations case										
	Actor					Evidence: open source			Evidence: interviews	
Name	Incumbent	Critic	Status-quo	Change Advocate	Political affiliation	Inquiry: Parliamenta	Inquiry: Expert	Media	Operational	Strategical
R. Plasterk	✓				PvdA	✓		✓	B+D	A
J. Hennis-Plasschaert	✓				VVD	✓			B+D	A
F. Timmermans	✓				PvdA	✓				
I. Opstelten	✓				VVD	✓				
G. Schouw		✓		✓	D66	✓				
L. Bontes		✓		✓	G. Bontes	✓				
R. Raak		✓		✓	SP	✓				
B. Ojik		✓		✓	GL	✓				
M. Thieme		✓		✓	PvdD	✓				
M. Bosma		✓		✓	PVV	✓				
M. Toorenburg		✓		✓	CDA	✓				
J. Recourt		✓	✓		PvdA	✓				
K. Dijkhoff		✓	✓		VVD	✓				
G. Segers		✓	✓		CU	✓				
R. Bisschop		✓	✓		SGP	✓				
N. Klein		✓		✓	50Plus	✓				
A. Pechtold		✓		✓	D66	✓				
E. Roemer		✓		✓	SP	✓				
G. Wilders		✓		✓	PVV	✓				
S. Buma		✓		✓	CDA	✓				
D. Samsom		✓	✓		PvdA	✓				
H. Zijlstra		✓	✓		VVD	✓				
A. Slob		✓	✓		CU	✓				
K. Staaij		✓	✓		SGP	✓				
L. Voortman		✓		✓	GL	✓				
B. de Winter		✓		✓	none	✓		✓	B	A

4.2.3 Crisis rhetoric and contest of framing

With the actors in the Snowden Revelations case in mind, it is now time to move to the crisis rhetoric they have used, as well as the frames that were being pushed. In the aftermath of the crisis, its causality (endogenous or exogenous) and significance (incident or a symptom) are focussed upon. This crisis-type language is used to frame the crisis as either a critical threat (type II) or a critical opportunity (type III).

Significance

In the Snowden Revelations, a clash on the significance of the crisis is seen between the contending actors. In this clash, some actors acknowledged the significance, but argued that it was an incident, whereas other actors have used crisis type rhetoric to maximize the significance of the event, arguing that it was a symptom.

In open source data, evidence for the first category, acknowledgement of the significance, whilst arguing that it is an incident, was found. An exemplifying situation is the speech in which Ronald Plasterk acknowledges the significance:

> "I found it of great importance to communicate that the Dutch intelligence service AIVD was not unlawfully collecting telecommunication data. However, I have also presented an alternative explanation, without knowing if this explanation was valid. The latter was of outstanding ill-judgement. I should not have done it. Therefore, I wish to offer my apologies." (2014a: 3:45:13).

In a later stage of the debate, Plasterk argues that the mistakes that were made were not illegal, and made with integrity, and that they will not be repeated (2014a: 4:06:24), framing the situation as an incident. Several of the actors agreed with this view, and have made similar interpretations. These actors include J. Hennis-Plasschaert（2014a: 06:04:38; 2014b: 4:45:45), J. Recourt (2014a: 41:55l 2014b: 1:33:45), G. Segers (2014a: 2:03:59; 2014b: 1:07:21) R. Bisschop (2014a: 2:09:18), K. Dijkhoff (2014a: 1:40:27; 2014b: 26:16), D. Samsom (2014a: 9:55:07), H. Zijlstra (2014a: 09:57:43), A. Slob (2014a: 9:59:23), and K. Staaij (2014a: 10:02:42). The evidence originating from the interview sources mostly supports this view, notably in interview A (39:12) and B (31:22).

The other actors made arguments that maximized significance, arguing that it was a symptom, rather than an incident. The most exemplary situation of this is the motion of no confidence, a 'motie van wantrouwen', that was issued by the leader of political party D66 Alexander Pechtold, with the signatories Roemer, Van Ojik, Thieme, Van Haersma Buma,

Klein, Wilders and Bontes. In this motion, it is suggested that the situation is an example of the structural failure and dysfunctionality of Minister Plasterk (2014a: 9:42:19). On multiple occasions, actors have offered the same, or similar, interpretations of the situation. This includes L. Voortman (2014b: 18:23), G. Schouw (2014a: 2:01; 2014b: 8:41), L. Bontes (2014a:16:09; 2014b: 1:19:57), R. Raak (2014a: 10:21; 2014b: 0:35), B. Ojik (2014a: 19:10), M. Thieme (2014a: 24:31), M. Bosma (2014a: 29:05; 2014b: 1:12:04), M. Toorenburg (2014a: 35:14; 2014b: 1:23:26) N. Klein （2014a: 2:13:49), E. Roemer (2014a: 9:44:53), G. Wilders (2014a: 09:50:05), and S. Buma (2014a: 09:53:04).

Causality

There is a clear clash on the causality of the crisis. Causality is characterized by actors who blame the crisis on either endogenous or exogenous factors. The months antecedent to the crisis, the Snowden revelations were kept from escalating by successful framing attempts to render the crisis causes exogenous, by focusing blame on the U.S. security and intelligence agencies. The pivotal moment in this is Ronald Plasterks' appearance in the news show 'Nieuwsuur', where he stated that the documents were collected and stored by the NSA, instead of the Dutch intelligence services (Nieuwsuur, 2013: 2.55). At the time, this was an assumption, rather than a fact, but it shifted the focus of the crisis to the debate of international intelligence cooperation, rather than to the discussion on the collection of metadata by the Dutch government. This statement later had to be rectified following a civil law suit, in a letter to parliament send on the 4th of February (NRC Handelsblad, 2014a). This rectification invoked a turning point, where the situation imploded to a crisis. In the parliamentary inquiry that followed, the crisis shifted from a focus on the collection of metadata on telecommunication by the Dutch intelligence services (the official topic of the debate), to the misleading of parliament and consequentially, the position of Minister Ronald Plasterk. This is best illustrated by the first statement in the debate, made by G. Schouw:

> "For the political party D66, one question is central today: has the Minister of Interior Ronald Plasterk adequately informed this chamber about the 1.8 million sets of telecommunication data?" (2014a: 2:01).

The critic actors unanimously agreed that this crisis had endogenous origins, and argued that it should have political repercussions. The status quo players and incumbent actors acknowledged the endogenous mistakes that were being made, but argued that these were made in accordance with the law, in accordance with integrity, and in the interest of the state (fe.

Zijlstra, 2014a: 9:57:53). This somewhat contradicts with the evidence found in the interview sources, most of them arguing that the crisis was exogenous.

Frames

The clash in causality and significance reflects clearly in types of frames that were seen in the aftermath of the Snowden revelations. Type II frames, predisposing the critical threat of the crisis to defend those agents responsible for this status quo and their respective policies; were frequently seen by the incumbent actors and status quo players. Type III frames are frequently pushed by critics and change advocates, arguing that the crisis predisposes a critical opportunity to change the current policies and/or that those in office should be held responsible, arguing for substantive reform or replacement in its entirety. This corresponds with the findings in the interview sources, in which it was argued that type II frames were the most dominant frames (interview A; B; C; D).

4.2.4 Exploitation arenas (media and inquiries)

This paragraph analyses the arena's in which the crisis exploitation predominantly took place. It answers the subquestion: *in which arenas was the exploitation of the crisis principally acted out?* The two arenas recognized in the theoretical framework, mass media and through official inquiry, are both analysed for the occurrence of actors employing crisis type rhetoric.

Mass media have played a vital role in the Snowden Revelations crisis. One reason of this is that they were the information channel chosen by Snowden, through the transmitting of files to investigative journalists at trusted media outlets. At this point, mass media became not only an arena, but also an actor as such in the exploitation game. This is especially seen abroad, where journalists such as Glenn Greenwald, Jacob Appelbaum, and Laura Poitras were actively involved interpreting the events, and communicating these events to a larger public. In the context of the Netherlands, and the crisis that occurred in response to the 1,8 million metadata files that were transmitted from the Netherlands to the US intelligence services, the arena of a mass media appeared to have had a pivotal role. In the open source analysis, on multiple occasions in multiple documents, it is suggested that Ronald Plasterks' appearance in the news show 'Nieuwsuur', wherein he falsely stated that the documents were collected by the NSA instead of the Dutch intelligence service (Nieuwsuur, 2013: 2.55), a statement which he later repeated in parliament on November 9th, causing the situation to diffuse (NRC Handelsblad, 2014a; 2014b; Kamerhandelingen 2014a). The rectification of these statements, made in the unannounced letter to parliament following the civil law suit, send on the 4th of February,

activated the most significant events in the second arena; the arena of official inquiry (Kamerbrief, 2014). As discussed in paragraph 4.2.2, there is some open source evidence found for framing attempts in online media, respectively by non-public actors, see also figure 5. No indication of successful framing attempts in other types of mass media were found.

In response to the rectification, parliament issued two emergency moments of official inquiry, in the form of a plenary debate consisting of the entire parliament, debating the question the situation and its consequences on the 9th and 11th of February (Kamerhandelingen 2014a; 2014b). Most of crisis' frame games are operated in these two moments. The second resulted in a confidence vote, a 'motie van wantrouwen', by the parliament in Ronald Plasterk, which failed to acquire a parliamentary majority. No expert-based inquiry was issued.

4.1.5 Actor propensities as a result of situational and temporal factors

This subchapter subjects the Snowden Revelations case to the situational and temporal factors that may shape the actor propensities. In terms of temporal factors, the political time of incumbency of the actors, and time to an upcoming election are measured. In the situational factors, a closer look at the sectoral compartmentalization is given.

The political time is characterized by a relatively new cabinet, that had become active on the 5th of November 2012, exactly 7 months before the first Snowden files were released on June 5th, 2013. In the in the multi-party electoral democracy of the Netherlands, cabinets serve for four consecutive years, which means that the next election was 33 months in the future, at the time that the situation became a crisis; the 4th of February 2014. In relative terms, 31% of the standard cabinet time had passed. In political time of incumbency, main incumbent actor Ronald Plasterk had been in a cabinet position for 51 months, in two terms. The other incumbent actors had been in cabinet office for 51 months (Timmermans), 37 months (Opstelten), and 15 months (Hennis-Plasschaert).

In terms of situational factors, concerning the scope of the crisis and its compartmentability, actor propensities were shaped as following. The crisis spanned four compartments within the Dutch governmental structure. First, and mainly, it hit the Ministry of Interior, which carries political responsibility for the intelligence services in the Netherlands, headed by Minister of Interior, Ronald Plasterk. Secondly, it concerned the Ministry of Defence, that was closely involved with the military intelligence service that eventually turned out to have collected the 1,8 million meta data files, Jeannine Hennis-Plasschaert. Thirdly, both the Ministry of Foreign Affairs, headed by Frans Timmermans, and the Ministry of Security and Justice, headed by Ivo Opstelten, were involved in the process of parliamentary inquiry

on, respectively, the topics of international intelligence cooperation and the legal framework of privacy. In total, this adds up to 4 governmental sectors. The crisis was never scaled up to the highest level of public responsibility, Prime-Minister Mark Rutte.

4.2.6 Policy, political and institutional impacts

This paragraph analyses the policy, political and institutional situation before the crisis, and compares it with the respective situations after the crisis. It answers the subquestion: *what impacts of the crisis are observable?* It is important to answer the question as a theory of crisis exploitation needs to capture how the clash between frames produces particular types of political and policy consequences. Following this logic, it is important to look at what has changed after a crisis, in relation to the situation before the respective crisis. Recalling the three spheres – policy, political and institutional – the situation before, in comparison with after, the crisis will be discussed for all three.

In terms of institutional effects, no evidence is found for any change in the aftermath of the Snowden Revelations crisis. There is little evidence suggesting the presence of a dispersed institutional field. Within the incipient field of cybersecurity, it appears that the actions of Plasterk drew all the focus of the crisis towards the governmental institution the represented, which is remarkable considering that the ministry of Defence was responsible for the meta data file collection, rather than the Ministry of Interior.

The policy sphere was subject to a discussion on three themes: the collection of metadata for national security purposes (Kamerhandeling, 2014a), cooperation with foreign security agencies (Kamerhandeling 2014b), and to a lesser extent, whistle-blower policy (Kamervragen, 2013c). Neither in the open source analyses, nor in the interviews, evidence is found for policy change on the latter two themes, in the aftermath of this crisis. However, on the first theme, significant policy changes have occurred since the Snowden Revelations crisis enveloped. In the parliamentary inquiry following the crisis, many actors pleaded against the mass collection of data, and against the collection of metadata in particular. Examples include statements by G. Schouw, (Kamerhandeling, 2014a: 2:01), R. Raak, (Kamerhandeling 2014a: 10:21), B. Ojik, (Kamerhandeling, 2014a: 19:10), M. Thieme (Kamerhandeling 2014a: 24:31). Other actors mentioned the prudent use of these techniques (fe. Bontes, Kamerhandeling, 2014a: 16:00). Despite the arguments made to the contrary, the collection of mass data was not limited, nor prohibited. Rather, the debate on the legal capabilities of the security and intelligence services continued, until it manifested itself in the 'Wet Inlichtingen en Veiligheidsdiensten 3', an update of the legal framework that was part of the coalition

agreements, initiated before the Snowden Revelations. Rather than limiting the legal capabilities of intelligence services, it did the exact opposite: it allowed for a "massive increase in legal competences" (NRC Handelsblad, 2017). The role that the Snowden crisis has played in this is unclear, but it does show that the parliamentary calls following the Snowden crisis had no, or a counterproductive, impact.

The final sphere is the main sphere that was influenced in the aftermath of the crisis: the political sphere. As discussed, due to attempts to exogenize the causes of the Snowden Revelations in his media and parliamentary appearance, which had gotten falsified following the civil action against him, much of the following parliamentary inquiry focussed on the position of Ronald Plasterk, within the political sphere. Many actors called for his resignation (fe. Wilders, Kamerhandelingen 2014a: 09:50:05), eventually leading to a vote of confidence. This vote acquired significant minority support, but failed to get a majority, as coalition parties VVD and PvdA, together with oppositional parties SGP and CU did not vote in favour, leaving the question of resignation up the incumbent himself. Although he did not resign, he did make amends for his previous actions, apologizing for his statements in Nieuwsuur, arguing that they were made based on integrity (NRC Handelsblad, 2014c). The above leads this thesis to conclude that in terms of political impacts, the crisis was successfully blamed on the incumbent, causing elite damage to the government in general, and Plasterk in particular. This open source analysis corresponds with findings in the interview sources (respondent B: 33:02).

4.2.7 Subconclusion Snowden Revelations

Summarizing, 26 actors that purposefully employed crisis type rhetoric to influence the consequences of the Snowden Revelations crisis were identified, 4 of which were incumbent actors, 21 of which were critic actors, and 1 of which was a non-public actor. In the contest of frames that occurred in the aftermath, a clash between type II and type III frames was observed, in which the crisis' significance was acknowledged by all, and maximized by some actors. Additionally, there was a majority of actors that interpreted the crisis as an incident, but this was heavily disputed by a minority group, that framed the crisis as a symptom of incompetency, which took form in a vote of confidence. Unsuccessful efforts were made by incumbent actors to exogenize the causes of the crisis. Non-public efforts helped endogenize the perceived causes of the crisis. In terms of arenas, it was furthermore observed that both the media and the inquiry arenas were significantly used in the contest of frames. Media framing attempts were found in both conventional and online media outlets, whereas there were two moments of political inquiry. No expert-based inquiry occurred. Furthermore, it was observed that the crisis

was situated far away from an election, and was broad in scope, spanning four governmental sectors and the second highest level of governmental responsibility. Additionally, the political time was characterized by a long period of incumbency (Plasterk). No evidence was found for institutional or policy impacts of the crisis. In the political sphere, blame was successfully focussed on the incumbent actor, causing elite damage to the Government in general, and to Ronald Plasterk in particular.

4.3 Case comparison

This subchapter offers a schematic and descriptive comparison of the findings resulting from the analysis conducted in the previous paragraphs of this chapter. When bringing all the empirical findings together, it can be found to which extend the Diginotar Hack and the Snowden revelations were wittingly exploited in the context of the cyber security domain of the Netherlands, and consecutively, which of the original mechanisms were active in this process. Furthermore, it can be found what similarities and differences both cases encompass. In chronological order, the original mechanisms are discussed, and visualized in figure 7.

Several types of actors were active in the exploitation of both cases: incumbents, critics, and in one instance, a non-public actor. In both cases a clash between type II and type III frames occurred, this clash being the most severe in the Snowden revelations case. The absence of severity in the frames clash within the Diginotar case can be explained by the ambiguity of the status quo: the status quo being a state of institutional, policy and political change. In both instances, a type II frame became the most dominant interpretation of the crisis case. Within the Snowden revelations case, this was heavily contested. In both cases, actors acknowledged the significance of the crisis and in both cases, it is found that critic actors, regardless of political affiliation, made attempts to maximize the significance of the event.

A difference is found in the causality efforts in the crisis-type rhetoric used by the contending actors. Although the hack occurred at a non-public company, within the Diginotar case, all actors recognized the causes of the crisis as endogenous: as originating from within the public sector and illustrating symptomatic vulnerability within the cyber management of this system. Again, this can be explained by an ambiguous status quo. In the Snowden case, a clear clash on causality was found between the incumbent and critic actors. The initial efforts to exogenize the crisis towards the NSA failed, which heavily strengthened critic efforts to endogenize the crisis. Incumbent actors furthermore framed the Snowden revelations crisis as

a ‘mistake out of integrity’, arguing that it was an incident, whereas critics argued that it was a symptom of political failure.

Furthermore, the cases deviated on the arena’s, with the Snowden case heavily published within the media arena, and little media activity concerning the Diginotar case. Remarkable was the actor-like role that the media arena had within the Snowden crisis, which made use of online media as a platform, alongside conventional methods. Diginotar saw both parliamentary and expert-based inquiries, whereas only parliamentary inquiry was found as an official arena of exploitation within the Snowden case. This could be the result of incumbent efforts to minimize the event. On temporal factors, both cases aligned, whereas on situational factors, the scope of the Snowden crisis was harder to compartmentalize, having more sectoral overlay.

In terms of impact, the Diginotar crisis occurred during a time of institutional transition. Responsibility for the crisis was predominantly taken by the original institution, and no evidence is found of a clash between institutions within this process. Because the core transition was already in motion before the crisis, it remains hard to attribute the institutional changes occurring in its aftermath to the crisis itself. However, anecdotal evidence suggests that the crisis strongly catalysed this change due to an increase in issue salience following the crisis. The strongest evidence for the impact of the Diginotar crisis is found in the policy sphere, where two core policy changes were directly attributable to the crisis. Within the political repercussions, the crisis had little: it rather showed evidence of diffused blame and elite escape.

In the Snowden crisis, the impact within the policy sphere is characterized by no, or arguably even counterproductive, policy change. No institutional change was found following the crisis, but in terms of institutional effects, the responsibility focussed on just one institution. This is remarkable as other institutions shared at least partial responsibility in the causes of the crisis. This can be explained by the political actions of the minister of this institution, which effectively focussed blame on himself. It also resulted in elite damage within the political sphere. Possibly, this difference in affected spheres of impact can be connected to the type of cyber crisis: the Snowden crisis being facilitated through the cyber domain, and the Diginotar crisis originating from the cyber domain.

The above constructs the empirical answer to the research question, by analysing its mechanisms. Herein, the main empirical finding is that in both cases, multiple purposeful attempts to exploit the cyber crises have occurred, both using the original, mechanisms of the model.

Figure 7: Case comparison

Case comparison		
Mechanism	Diginotar	Snowden Revelations
Crisis	Type I cyber crisis	Type II cyber crisis
Actors	12 actors: 2 incumbent actors, 10 critic actors	26 actors: 4 incumbent actors, 21 critic actors, 1 non-public
Rhetoric: significance	Acknowledged & maximized	Acknowledged & maximized
Rhetoric: causality	Endogenous & symptom	Exogenous & endogenous efforts + incident & symptom
Frames	Type II	Type II
Arena: media	Some conventional	Conventional & online
Arena: official inquiry	Parliamentary & expert-based	Parliamentary
Factors: situational	Narrow and shallow scope	Broad and shallow scope
Factors: temporal	Long period of incumbency (96) & long period to next election (40 months)	Long period of incumbency (51 months) & long period to next election (33 months)
Impacts: institutional	Possible core change	None
Impacts: Political	Diffused blame & elite escape	Focused blame & elite damage
Impacts: Policy	Core change	None

5. Reflection

With the summary of the empirical results that concluded the previous chapter in mind, this thesis can commence with an informed debate on the implications of these findings, in this final chapter. Firstly, it will give context to the empirical findings in subchapter 5.1. In doing so, it will formulate a conclusive answer to the research question of this thesis. Following, it will discuss what societal implications these findings have, which are linked to policy recommendations in subchapter 5.2, for those who seek to use the acquired knowledge in practice. This thesis will conclude with a discussion of the broader scientific relevance, resulting in research options and recommendations for further study in subchapter 5.3.

5.1 Result conclusion

This study conducted a theory building research to the crisis exploitation model by Boin, 't Hart and McConnell (2009), where it looked at the effects that a new form of crisis, the cyber crisis, has on the mechanisms of this model. The deviant characteristics of the cyber domain showed potential implications for the mechanisms of the model, most notably through its actor relevancy, additional arena, and its volatile incipiency. In its analysis, this research furthermore answered the academic call to broaden and deepen the research of the crisis exploitation model. This was done through a case study of the two main cyber crises in the context of the Dutch cyber domain. These cases displayed a large comparative variation, making them suitable for a most different case study model. Both cases, the Diginotar Hack and the Snowden Revelations, were subjected to the research question: *Are the Diginotar Hack and the Edward Snowden revelations wittingly exploited in the context of the cyber security domain of the Netherlands, and if so, through which mechanisms?*

Generally, in both cases, evidence of multiple purposeful attempts to influence the cyber crises are found, and, therefore, the first part of the research question can be answered with: yes, the Diginotar Hack and the Edward Snowden revelations are wittingly exploited in the context of the cyber security domain of the Netherlands. Providing this answer with context, this means that, like conventional crises, the new phenomenon of cyber crises can be, and are, exploited. Based on the studied cases, this holds true for both crises occurring in, and cases facilitated through, the cyber domain.

The answers to the second part of the research question, *through which mechanisms*, essentially looks at how the characteristics of the cyber domain influence the original mechanisms of the exploitation model. From the analysis of the cyber domain it was concluded

that non-public actors could have a large(r) role in crisis exploitation; the contest of frames could occur in the new form of online media, and due to the incipiency of the domain, the impacts of the crisis could be more volatile.

For the first of these implications, the Diginotar and Snowden cases show limited evidence. In the Diginotar hack, actors from the private sector appeared to have a role in the aftermath of the crisis, notably through the IRB and CSR institutions, but this was a background role at most. The Snowden case showed some additional support for this implication, in the form of a civilian that had a pivotal role in the development of the crisis, and a participating role in the contest of frames. For the second implication of an additional media arena, online media, no evidence was found in the Diginotar case, but some evidence of its presence was found in the Snowden case, notably through twitter and blogposts. However, as argued in the notes for further study, analysing the content in the online media arena proofed to be a difficult task. For the third implication, the volatile incipiency, some evidence of influence is found. Particularly in the Diginotar case, the policy and institutional sphere were volatile, and evidence is found that this manifested in the impact of the crisis. Sidenotes to this are that the role of the crisis in the institutional sphere is not entirely sure, as some of the institutional change was planned before the crisis occurred; and the paradox that in all impact spheres, the status quo is characterized by a changing environment, causing it to be dispersed.

In the Diginotar crisis, the causes of the crisis were perceived as endogenous, the incumbent had spent a long time in office, there was little media coverage other than one press conference, the elections were far away, and the main locus of inquiry was expert based. Of the five factors contributing to the success rate of oppositional forces, only the first and second factors align. Therefore, the impact of the crisis is probably best explained by the willingness of the incumbents to change the current policy and institutions, rather than the oppositional attempts to compel these. The Snowden crisis case was predominantly perceived as endogenous, the incumbent was in office for a long time, the next election was far away, there was a lot of negative media attention surrounding the case, and the main locus of inquiry was parliamentary inquiry. Out of the five factors contributing to oppositional success, only the election factor does not align in the Snowden case. It is therefore remarkable that the impact of the crisis was very limited, having no institutional impact; no, or even counterproductive, policy impact, and nothing other than reputation damage in terms of political impact for the incumbent.

These findings implicate the following. The model of crisis exploitation is relevant and present within the cyber crisis; a new form of crises. The original mechanisms of crisis exploitation were actively found in the researched cases, and in the instances of online media and volatile incipiency, these mechanisms were, at least partially, influenced by the characteristics of the cyber domain. Furthermore, it is remarkable that in the impact spheres, the researched cases did not follow the trends for oppositional success observed in the original model. Some, but limited, support was found to connect these to the implications that the characteristics of cyberspace impose on these mechanisms. Consequently, this implies that within the exploitation of cyber crises, based on the two cases researched, conventional methods and conditions of exploitation are not sufficient for oppositional success.

5.2 Policy recommendation

Translating the findings of this thesis to practical policy recommendations, this thesis provides support for the assumption that a crisis can make or break a career, policy or even institute. Because of the changed actor dynamic, policy makers should be attentive to actors originating from other sectors than the public sector, participating in the contest of frames. This is important because, in contrast with public actors, those actors are not the direct or indirect product of democratic elections, but could rather serve singular interests. An example could be an actor from the private sector pushing for a larger market share, or an individual with a rejectible world view. In a worst-case scenario, these are forces for a larger societal division, that is less fair than the system we are currently used to.

Furthermore, new technologies change the ways of communication, perhaps outdating established forms of political communication. It is likely that in the crises to come, the role of alternative arenas will intensify, as was limitedly exemplified in the Snowden crisis case. In policy, this changed dynamic should be taken into account, but judging from the most recent U.S. elections, this idea has already landed.

Finally, at this moment, the cyber domain is still in an incipient stage. The Diginotar case proved the volatility of, especially, the policy domain, but this was also seen in the institutional domain. A policymaker realizing this, might be more influential than a policymaker that does not.

5.3 Recommendation for further study

In the introductory remarks, this thesis claimed that studying cyber crises is a useful occupation, because of its the expected growth in occurrence and significance. Proof of this

was found before the thesis was even finished. In May 2017, the Wannacry ransomware caused a crisis-like situation when it attacked and paralyzed several systems in the vital infrastructure, including hospitals. Not one month later, a related piece of malware, called Petya, specifically attacked energy companies and the power grid in Ukraine, including the radiation monitoring system of the defunct Chernobyl nuclear power plant. Both made use of vulnerabilities in Microsoft, that the U.S. intelligence community was aware of, but kept a secret because it was used for intelligence purposes. The fact that this is a legal occupation, also in the Netherlands, as it is used in police hacking, stirred a debate to the modus operandi of intelligence services and their role in cyber security. At the moment of writing, the thesis had a deficiency in the amount of (type I) cases it could use. In fact, the Diginotar case was the only undisputed crisis case in the context of the Netherlands. Future study should take note of new occurrences of cyber crises. Enlarging the number of analysed cases will add to the strength of the findings in this thesis, or perhaps falsify them. In this study, the conclusions are based on a very low number of cases, and a very low number of occurrences within these cases. There are some promising implications for the model of crisis exploitation, that are the product of the in-depth analysis this study has conducted, but the academic value of these findings would significantly increase from additional applications.

In addition, due to its sheer size, analysing the content in the online media arena in its entirety proofed to be a task beyond the capabilities of this thesis. Further study could benefit from new techniques of big data analysis to make researching this arena in the future more viable.

Bibliography

Academic publications

Alink, F., Boin, R.A. and ’t Hart, P. (2001) ‘Institutional crises and reforms in policy sectors: the case of refugee policy in Europe’, Journal of European Public Policy 8(2): 286–306.

Alink, F. B. (2006). *Crisis als kans? Over de relatie tussen crises en hervormingen in het vreemdelingenbeleid van Nederland en Duitsland*. Vossiuspers UvA.

Ansell, C., Boin, A. and Kuipers, S. (2016). 22. Institutional crisis and the policy agenda. In Nikolaos Zahariadis (eds). *Handbook of Public Policy Agenda Setting*, Edward Elgar publishing. 415 - 432.

Antonopoulos, A. M. (2017). ‘Blockchain vs. Bullshit: Thoughts on the Future of Money’. from https://www.youtube.com/watch?v=SMEOKDVXlUo. Published on 2017, April 22. Keynote talk at the Blockchain Africa Conference on March 2nd, 2017 Johannesburg, South Africa. Retrieved June 20, 2017.

Baumgartner, F.R. and Jones, B.D. (1993). Agendas and Instability in American Politics, Chicago: University of Chicago Press.

Birkland, T.A. (1997). After Disaster: Agenda Setting, Public Policy and Focusing Events, Washington, DC: Georgetown University Press.

Birkland, T.A. (2006). Lessons of Disaster: Policy Change After Catastrophic Events, Washington, DC: Georgetown University Press.

Boeke S. (2016). First Responder or Last Resort? The role of the Ministry of Defence in national cyber crisis management in four European countries. Den Haag: Universiteit Leiden.

Boin, A. P.'t Hart, E. Stern and B. Sundelius. (2017). The Politics of Crisis Management. Public Leadership under Pressure. (2nd edition). Cambridge University Press: Cambridge.

Boin, A., 't Hart, P. and McConnell, A. (2009). Crisis exploitation: political and policy impacts of framing contests. *Journal of European Public Policy*, *16*(1), 81-106.

Boin, A. and McConnell, Allan and Hart, P. (2008) *Conclusions: The Politics of Crisis Exploitation.* In: Governing after crisis: the politics of investigation, accountability and learning. Cambridge University Press, Cambridge. 285-316.

Bovens, M. and t'Hart, P. (1996) Understanding Policy Fiascos. New Brunswick: Transaction Publishers.

Brandstrom, A. and Kuipers, S. (2003). 'From ''Normal Incidents'' to Political Crises: Understanding the Selective Politicization of Political Failures', *Government and Opposition* 38(3): 279–305.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43-62.

Chourci, N. (2014). MIT ECIR 2014: Interview by the CUBE Media. Accessed on March the 12th of 2017, https://www.youtube.com/watch?v=Kc9SZ2hpWSU.

Clark, D. (2010). Characterizing cyberspace: past, present and future. *MIT CSAIL, Version*, *1*, 2016-2028.

Clunan, A. and Trinkunas, H. A. (2010). *Ungoverned spaces: Alternatives to state authority in an era of softened sovereignty*. Stanford University Press.

Cremin, K. M. (2011). Challenges to institutionalization: The definition of Institution and the future of Olmstead litigation. *Tex. Journal. on CL & CR*, 17(6).

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. (3rd ed.) Sage publications.

Dunn-Cavelty, M. (2016). Cyber-Security. in Collins, A. (eds). *Contemporary security studies*. 4th ed. Oxford University Press. 400 - 407.

Entman, R. (1993) 'Framing: toward clarification of a fractured paradigm', Journal of Communication 43(4): 51–8.

Gerring, J. (2007). Case Study Research: Principles and Practices. Cambridge University Press: Cambridge.

Gude, H., Poitras, L. and Rosenbach, M. (2013, August 05). Mass Data: Transfers from Germany Aid US Surveillance - SPIEGEL ONLINE - International. Retrieved July 2, 2017, from http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html

't Hart, P. (2009). Summary of 15 Crisis Management Cases. *Unofficial publication on former personal website, accessible through WayBackMachine*: https://web.archive.org/web/20090912073358/http://polsc.anu.edu.au/staff/hart/pubs/SUMMARY_OF_15_CRISIS_MANAGEMENT_CASES_FOR_JEPP_ARTICLE.pdf.

Hansel, M. (2016). Cyber-attacks and psychological IR perspectives: explaining misperceptions and escalation risks. *Journal of International Relations and Development*, 1-29.

Inkster, N. (2014). The Snowden revelations: Myths and misapprehensions. *Survival*, *56*(1), 51-60.

Johnson, L. K., Aldrich, R. J., Moran, C., Barrett, D. M., Hastedt, G., Jervis, R., and Wark, W. K. (2014). An INS Special Forum: Implications of the Snowden Leaks. *Intelligence and National Security*, *29*(6), 793-810.

Keeler, J. T. (1993). Opening the window for reform: Mandates, crises, and extraordinary policy-making. *Comparative Political Studies*, *25*(4), 433-486.

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, *38*(2), 7-40.

Kingdon, J. (1984) Agendas, Alternatives, and Public Policies. New York: HarperCollins.

Kuipers, S. (2006) The Crisis Imperative: Crisis Rhetoric and Welfare State Reform in Belgium and the Netherlands in the Early 1990s. Amsterdam University Press: Amsterdam.

McCombs, M. E. and Shaw, D. L. (1972). The agenda-setting function of mass media. *Public opinion quarterly*, *36*(2), 176-187.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Nohrstedt, D. and Weible, C. M. (2010). The logic of policy change after crisis: Proximity and subsystem interaction. *Risk, Hazards & Crisis in Public Policy*, *1*(2), 1-32.

Naughton, J. (2001). Contested space: the internet and global civil society. *Global civil society*, 147-168.

Olsson, E. K., Nord, L. W. and Falkheimer, J. (2015). Media coverage crisis exploitation characteristics: A case comparison study. *Journal of Public Relations Research*, *27*(2), 158-174.

Ottis, R., and Lorents, P. (2010). Cyberspace: Definition and implications. In *International Conference on Information Warfare and Security* (p. 267). Academic Conferences International Limited.

Proschinger, C. (2012). StuxNet, AnonAustria, DigiNotar & Co: What they teach us about operating IT systems in a secure way. Accessible at: https://www.econstor.eu/bitstream/10419/60354/1/720907926.pdf

Quarantelli, E. L. (2005). Catastrophes are different from disasters: some implications for crisis planning and managing drawn from Katrina. *Understanding Katrina: Perspectives from the social sciences*.

Rosenthal, U., Boin, R.A. and Comfort, L.K. (eds) (2001) Managing Crises: Threats, Dilemmas, Opportunities, Springfield, IL: Charles C. Thomas.

Rosenthal, U. and 't Hart, P. and Charles M.(1989) "The World of Crises and Crisis Management" in Coping With Crises: The Management of Disasters, Riots, and Terrorism. 3-33. Springfield, Illinois: Charles C. Thomas.

Sabatier, P.A. (ed.) (1999) Theories of the Policy Process, Boulder, CO: Westview Press.

Seeger, M.W., Sellnow, T.L. and Ulmer, R.R. (2003) Communication and Organizational Crisis, Westport, CT: Praeger.

Singer, P. W. and Friedman, A. (2014). *Cybersecurity: What Everyone Needs to Know*. Oxford University Press.

Trump, D.J. [ABC15 Arizona]. (2016, September 6th). *Donald Trump talks Cyber Terror - ISIS - National Security Threats.* [Video File]. Retrieved from https://www.youtube.com/watch?v=ab5QOgNqcxU&index=365&list=LLxkWpjgILlFsZJ_3a89-Klw.

Tsagourias, N. (2016). Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts. *Journal of Conflict and Security Law*, krw020.

Ulmer, R. R., Sellnow, T. L. and Seeger, M. W. (2013). *Effective crisis communication: Moving from crisis to opportunity*. (3rd edition). Sage Publications.

Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Warner, M. (2012). Cybersecurity: a pre-history. *Intelligence and National Security*, *27*(5), 781-799.

Washington Post. (2017). *Analysis | One of the most important lessons of the crippling ransomware crisis*. Washington Post. Retrieved 18 May 2017, accessible at https://www.washingtonpost.com/news/the-switch/wp/2017/05/12/one-of-the-most-important-lessons-of-the-crippling-malicious-software-crisis/?utm_term=.1d4a6a36bb40

Wright, D. and Kreissl, R. (2013). European responses to the Snowden revelations: A discussion paper. Accessible at: http://www.irks.at/en/assets/irks/Publikationen/Unterlagen/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf

Open source publications

@brenno. (2013a) Volgens Plasterk zijn er geen gesprekken afgeluisterd: […] en het OM doet *geen* onderzoek naar NSA-schandaal [Tweet]. Brenno de Winter, 31 October 2013. Retrieved from https://twitter.com/brenno/status/396016938117525504.

@brenno. (2013b) Oh jee. Ronald Plasterk is bamg. Net geweigerd door BZK voor persconferentie over eID [Tweet]. Brenno de Winter, 19 December 2013. Retrieved from https://twitter.com/brenno/status/413594322958057473.

CSBN 1. (2011). Cybersecuritybeeld Nederland 2011. *Ministerie van Veiligheid en Justitie*. https://www.rijksoverheid.nl/documenten/rapporten/2011/12/25/cybersecuritybeeld-nederland-december-2011.

CSBN 3. (2013). Cybersecuritybeeld Nederland 2013. *Ministerie van Veiligheid en Justitie*. https://www.rijksoverheid.nl/documenten/kamerstukken/2013/07/03/cybersecuritybeeld-nederland.

CSBN 4. (2014). Cybersecuritybeeld Nederland 2014. *Ministerie van Veiligheid en Justitie*. https://www.rijksoverheid.nl/documenten/wob-verzoeken/2014/08/27/cybersecuritybeeld-nederland-nummer-4.

Inspectie Veiligheid en Justitie. (2012). Evaluatie van de rijkscrisisorganisatie tijdens de Diginotar-crisis. https://www.rijksoverheid.nl/documenten/rapporten/2012/06/28/evaluatie-van-de-rijkscrisisorganisatie-tijdens-de-diginotar-crisis.

GCCS. (2015). International Case Report on Cyber Security Incidents. *Global Conference on Cyber Space.* https://www.gccs2015.com/sites/default/files/documents/ICR_CYBERCECURITYINCIDENTS_LR.PDF.

Kabinetsreactie. (2013). Kabinetsreactie op onthullingen Edward Snowden. *Ministeries van VenJ, BZK, Def en BZ naar Tweede kamer der Staten-Generaal*. 14-09-2013.

https://www.rijksoverheid.nl/documenten/kamerstukken/2013/09/14/kabinetsreactie-op-onthullingen-edward-snowden

Kamerbrief. (2011a). Kamerbrief digitale inbraak. DigiNotar. *Ministeries van VenJ en BZK, naar Tweede kamer der Staten-Generaal*. 16-09-2011. https://www.rijksoverheid.nl/documenten/kamerstukken/2011/09/16/kamerbrief-digitale-inbraak-diginotar

Kamerbrief. (2011b). Kamerbrief DigiNotar-problematiek. *Ministerie van BZK, naar Tweede kamer der Staten-Generaal*. 05-12-2011. https://www.rijksoverheid.nl/documenten/kamerstukken/2011/12/06/kamerbrief-diginotar-problematiek

Kamerbrief (2011c). Informatie- en communicatietechnologie (ICT); Brief regering; Stand van zaken moties Diginotar en ICT-problemen bij de overheid. *Tweede kamer der Staten-Generaal*. 14-11-2011. https://zoek.officielebekendmakingen.nl/kst-26643-214.html

Kamerbrief. (2012). Kamerbrief over DigiNotar onderzoeken. *Ministerie van BZK, naar Tweede kamer der Staten-Generaal.* 16-03-2012. https://www.rijksoverheid.nl/documenten/kamerstukken/2012/03/16/kamerbrief-over-diginotar-onderzoeken

Kamerbrief. (2013a). Gegevensbescherming en PRISM. *Ministerie van VenJ naar Eerste kamer der Staten-Generaal*. 02-10-2013. https://www.rijksoverheid.nl/documenten/kamerstukken/2013/10/03/gegevensbescherming-en-prism

Kamerbrief. (2013b). Kamerbrief inzake reactie NSA onderschepte 1,8 miljoen telefoontjes. *Ministerie van BZK naar Tweede kamer der Staten-Generaal*. 28-10-2013. https://www.rijksoverheid.nl/documenten/kamerstukken/2013/10/28/brief-aan-tk-inzake-reactie-bericht-nsa-onderschepte-18-miljoen-telefoontjes

Kamerbrief. (2013c). Brief van minister Plasterk (BZK) aan de Tweede Kamer over NSA. *Naar Tweede kamer der Staten-Generaal*. 31-10-2013.

https://www.rijksoverheid.nl/documenten/kamerstukken/2013/10/31/brief-van-minister-plasterk-bzk-aan-de-tweede-kamer-over-nsa.

Kamerbrief. (2013d). Kamerbrief over de werkwijze van de Amerikaanse National Security Agency (NSA). *Ministerie van BZK naar Tweede kamer der Staten-Generaal*. 05-11-2013. https://www.rijksoverheid.nl/documenten/kamerstukken/2013/11/05/kamerbrief-over-de-werkwijze-van-de-amerikaanse-national-security-agency-nsa.

Kamerbrief. (2014). Berichtgeving in Der Spiegel. *Ministerie van BZK naar Tweede kamer der Staten-Generaal*. 04-02-2014. https://www.scribd.com/document/204782437/Kamerbrief-Met-Reactie-Op-Berichtgeving-Metadata-Telefoonverkeer.

Kamerbrief. (2015). Kamerbrief reactie op het interview van de heer Snowden. *Ministeries van BZK en Def naar Tweede kamer der Staten-Generaal*. 06-02-2015. https://www.rijksoverheid.nl/documenten/kamerstukken/2015/02/06/kamerbrief-reactie-op-het-interview-van-de-heer-snowden.

Kamerhandelingen. (2011). Plenair debat over Diginotar en ICT-problemen bij de overhead. *Tweede kamer der Staten-Generaal.* 13 oktober 2011. http://2ekmr.nl/wPc.

Kamerhandeling. (2014a). Verzamelen metadata telefoonverkeer door Nederlandse veiligheidsdiensten. *Tweede kamer der Staten-Generaal.* 11-02-2014. https://zoek.officielebekendmakingen.nl/h-tk-20132014-52-18.html.

Kamerhandeling. (2014b) Afluisteren door de NSA. *Tweede kamer der Staten-Generaal.* 9-02-2014. https://zoek.officielebekendmakingen.nl/h-tk-20132014-73-8.html.

Kamerstuk. (2012). Algemeen Overleg Informatie- en communicatietechnologie (ICT). *Tweede kamer der Staten-Generaal*. 22 maart 2012. https://zoek.officielebekendmakingen.nl/kst-26643-229.html.

Kamervragen. (2011a). Een blunder bij Diginotar. *Tweede kamer der Staten-Generaal*. 01-09-2011. https://www.rijksoverheid.nl/documenten/kamerstukken/2011/09/01/een-blunder-bij-diginotar.

Kamervragen. (2011b). Beantwoording Kamervragen internetcertificaten, beveiliging van DigiD en overheidswebsites, en DigiNotar. *Ministeries van VenJ en BZK, naar Tweede kamer der Staten-Generaal.* 13-09-2011. https://www.rijksoverheid.nl/documenten/kamerstukken/2011/09/13/beantwoording-kamervragen-internetcertificaten-beveiliging-van-digid-en-overheidswebsites-en-diginotar.

Kamervragen. (2011c). Internetcertificaten. *Tweede kamer der Staten-Generaal*. 31-08-2011. https://zoek.officielebekendmakingen.nl/kv-tk-2011Z16610.html.

Kamervragen. (2011d). De beveiliging van Digi-D en overheidswebsites. *Tweede kamer der Staten-Generaal*. 31-08-2011. https://zoek.officielebekendmakingen.nl/kv-tk-2011Z16612.html.

Kamervragen. (2011e). Vragen van het lid Gesthuizen aan de minister van Binnenlandse Zaken en Koninkrijksrelaties over het bericht "Rijk toch bezorgd over hack DigiNotar" (mondelinge vragenuur). *Tweede Kamer der Staten-Generaal*. 6 september 2011. https://zoek.officielebekendmakingen.nl/h-tk-20102011-102-7.html.

Kamervragen. (2012). Beantwoording Kamervragen over DigiNotar. *Ministerie van EZ, naar Tweede kamer der Staten-Generaal*. 14-12-2012. https://www.rijksoverheid.nl/documenten/kamerstukken/2012/12/14/beantwoording-kamervragen-over-diginotar.

Kamervragen. (2013a). Beantwoording Kamervragen over DigiNotar-affaire op basis van WOB-stukken. *Ministeries van VenJ, BZK en EZ, naar Tweede kamer der Staten-Generaal.* 28-05-2013. https://www.rijksoverheid.nl/documenten/kamerstukken/2013/05/28/beantwoording-kamervragen-over-diginotar-affaire-op-basis-van-wob-stukken.

Kamervragen. (2013b). Kamerbrief met kabinetsreactie op ingediende moties NSA. *Ministerie van BZK naar Tweede kamer der Staten-Generaal*. 31-10-2013. https://www.rijksoverheid.nl/documenten/kamerstukken/2013/10/31/kamerbrief-met-kabinetsreactie-op-ingediende-moties-nsa.

Kamervragen. (2013c). Beantwoording Kamervragen over een bezoek van klokkenluider Snowden aan de Tweede Kamer. *Ministerie van VenJ, naar Tweede kamer der Staten-Generaal.* 07-11-2013. https://www.rijksoverheid.nl/documenten/kamerstukken/2013/11/09/antwoorden-kamervragen-over-een-bezoek-van-klokkenluider-snowden-aan-de-tweede-kamer.

Kamervragen. (2014). Beantwoording vragen inzake berichtgeving in NRC Handelsblad dat Nederland doelwit is geweest van NSA. *Ministerise van BZK en Def, naar Tweede kamer der Staten-Generaal.* 13-01-2014. https://www.rijksoverheid.nl/documenten/kamerstukken/2014/01/13/beantwoording-vragen-inzake-berichtgeving-in-nrc-handelsblad-dat-nederland-doelwit-is-geweest-van-nsa.

Kamervragen. (2015). Beantwoording Kamervragen over de uitlatingen Snowden over Nederland en de NSA. *Ministerise van BZK en Def, naar Tweede kamer der Staten-Generaal.* 06-02-2015. https://www.rijksoverheid.nl/documenten/kamerstukken/2015/02/06/beantwoording-kamervragen-over-de-uitlatingen-van-snowden-over-nederland-en-de-nsa.

NCSS 1. (2011) The National Cyber Security Strategy (NCSS): Success Through Cooperation. Ministerie van Veiligheid en Justitie. The Hague, Netherlands, http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011.

NCSS 2. (2013) The National Cyber Security Strategy 2: From awareness to capability. Ministerie van Veiligheid en Justitie. The Hague, Netherlands, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf.

NOS. (2011). Persconferentie Donner over Diginotar. *Nederlandse Publieke Omproep*. Video file, total duration 26:13 minutes. Date of publication 06-09-2011. http://nos.nl/video/270276-persconferentie-donner-over-diginotar.html.

NRC Handelsblad. (2011). Een mooie dag voor een black-out. *Marc Hijink and Steven Derix*. 10 September 2011. https://www.nrc.nl/nieuws/2011/09/10/een-mooie-dag-voor-een-black-out-12034434-a1094965.

NRC Handelsblad (2013). *'NSA maakte gebruik van hack IT-bedrijf DigiNotar'.* Auhor: Marc Hijink. Date of publication: 14-09-2013. Accessible at: https://www.nrc.nl/nieuws/2013/09/14/nsa-maakte-gebruik-van-hack-it-bedrijf-diginotar-a1431586.

NRC Handelsblad (2014a). 18 miljoen records tegen terreur. *NRC Handelsblad online*. 4 February 2014 Available at: https://www.nrc.nl/nieuws/2014/02/06/18-miljoen-records-tegen-terreur-1346467-a934431.

NRC Handelsblad (2014b). Hoe Plasterk verstrikt raakte in NSA affaire – een beknopte tijdslijn. 6 February 2014. *NRC Handelsblad online*. Available at: https://www.nrc.nl/nieuws/2014/02/06/hoe-plasterk-verstrikt-raakte-in-nsa-affaire-een-beknopte-tijdlijn-a1427394.

NRC Handelsblad. (2014c). Brede steun motie van wantrouwen, maar Plasterk treedt niet af. *NRC Handelsblad online*. 12 februari 2014. Available at https://www.nrc.nl/nieuws/2014/02/12/brede-steun-motie-van-wantrouwen-maar-plasterk-treedt-niet-af-a1427255?utm_source=NRC&utm_medium=banner&utm_campaign.

NRC Handelsblad. (2017). Met een sleepnet door het internet op zoek naar terroristen. NRC Handelsblad. 12 July 2017. Available at: https://www.nrc.nl/nieuws/2017/07/12/met-een-sleepnet-door-het-internet-op-zoek-naar-terroristen-6580813-a1544813.

Onderzoeksraad Voor Veiligheid. (2012). Het DigiNotarincident. *Onderzoeksraad Voor Veiligheid*. 28-06-2012. Accessible at:

https://www.onderzoeksraad.nl/nl/onderzoek/1094/het-diginotarincident/fase/1120/onderzoek-diginotar-richt-zich-op-digitale-veiligheid-overheid#fasen.

Rijksauditdienst. (2012) Rapport RAD-onderzoek 'DigiNotar'. *Ministerie van Financien.* 16-03-2012. https://www.rijksoverheid.nl/documenten/rapporten/2012/03/16/rapport-rad-onderzoek-diginotar.

TPO. (2013). Waarom ook ik de Staat aanklaag. *The Post Online.* 06-11-2013 http://politiek.tpo.nl/column/waarom-ook-ik-de-staat-aanklaag/.

VPRO. (2013). Brenno de Winter en de boodschap achter de daging van Plasterk. 6 november 2013. Retrieved from https://www.vpro.nl/speel~POMS_VPRO_423799~brenno-de-winter-en-de-boodschap-achter-de-daging-van-plasterk~.html.

Appendices

Appendix A: Overview Interviews

As agreed upon with the respondents, names of the respondents are anonymized in the version of this thesis that is publicly available.

Number	Name	Category	Date	Status
A	Name omitted	Policy	04-01-17	Conducted
B	Name omitted	Operative	16-01-17	Conducted
C	Name omitted	Policy	03-02-17	Conducted
D	Name omitted	Operative	10-02-17	Conducted

Appendix B: Standardized interview guide

Interview guide (English)

Introductory remarks

1. Goal of the interview

This interview is conducted in reference to a master thesis at the Leiden University, as a part of the study of *Crisis and Security Management*. The subject of the research is the consequences of crisis situations in the public order. Within this subject, a public administration theory to crisis exploitation is applied and tested to two cases of crisis within the cyber domain: the Diginotar crisis of 2011 and the Snowden revelations crisis in 2013. The following interview will discuss both cases.

2. Confidentiality

With your consent, this interview is recorded. The recorded material will be interpreted by the researcher and processed as data in the analysis of the research. The interview is one in a series of interviews. Statements will only be cited if they deviate from a trend or if they are specifically exemplary of a trend. This will be done anonymously.

3. Format interview

The type of interview that is being conducted is a standardized, open-ended interview, which means that it uses the same questions in every interview for the purpose of comparability. In some instances, follow up questions can be asked by the interviewer. The interview consists of two generally equal parts, corresponding with the cases studied in the research and will roughly take about 30 minutes.

Questions Diginotar Case

A crisis is a disruption of social routines and expectations. It is often characterized by a situation of urgency, threat, and insecurity. The first case of crisis that is being researched is the Diginotar crisis of 2011, consisting of the situation that developed after it was publicized that the firm Diginotar, issuing trusted website certificates, was hacked, making the certificates they issued, and the government services that relied on them, insecure.

1. Within the definition as used above, do you consider the Diginotar hack of 2011 a crisis-situation?

2. What was your function when the Diginotar hack became public?

3. What was your role during and after the crisis (situation) that followed?

Contest of frames

During and after a crisis, those involved seek explanations. Theoretically, there are three possible responses to a crisis: denying that it is a crisis, explaining the crisis as a critical threat to the status quo, and explaining the crisis as a critical opportunity to change the status quo.

4. In your opinion, which of these three options is most apt in explaining the situation that developed during the Diginotar crisis?

5. Were there other people involved that clearly explained the crisis in one of the other options?

6. Generally, was the crisis explained as an incident or as a symptom of something bigger?

Policy change

It is argued that crises open a window of opportunity for those seeking to exploit it. In this sense, a crisis can trigger reform. The policy situation before the Diginotar crisis is already characterized by reform, including the drafting up of a national cyber security strategy and the relocating of the cyber organization from the Ministry of interior to the Ministry of Security and Justice.

7. In your opinion, do you see an alteration in the direction of policy after the Diginotar crisis occurred?

8. Could this alteration (partially) be explained by the Diginotar crisis?

9. Do you see any institutional reform as a result of the Diginotar crisis?

Position of office-holders

In the period preceding the Diginotar crisis, the organization of cyber security within the Dutch government was undergoing a transition from the minister of interior (Piet Hein Donner) to the minister of security and justice (Ivo Opstelten).

10. If any, which office-holders were held accountable as a consequence of the crisis?

11. Did they accept this responsibility in your opinion?

12. Did the crisis influence the position of other office-holders to any extent?

13. Did the media influence this process?

Questions Snowden Revelations Case

A crisis is a disruption of social routines and expectations. It is often characterized by a situation of urgency, threat, and insecurity. The second case of crisis that is being researched is the crisis that developed in 2013, after Edward Snowden revealed the depth and width of the U.S. intelligence and security occupations. The extent to which new technologies used to monitor populations all over the world lead to global outrage.

1. Within the definition as used above, did the Snowden revelations of 2013 a crisis within Dutch government?

2. What was your function when this situation took place?

3. What was your role during and after the crisis (situation) that followed?

Frame games

During and after a crisis, those involved seek explanations. Theoretically, there are three possible responses to a crisis: denying that it is a crisis, explaining the crisis as a critical threat to the status quo, and explaining the crisis as a critical opportunity to change the status quo.

4. In your opinion, which of these three options is most apt in explaining the situation that developed during the Edward Snowden Revelations?

5. Were there other people involved that clearly explained the crisis in one of the other options?

6. Generally, was the situation explained as an incident or as a symptom of something bigger?

Policy change

It is argued that crises open a window of opportunity for those seeking to exploit it. In this sense, a crisis can trigger reform.

7. In your opinion, do you see an alteration in the direction of policy after the Edward Snowden crisis occurred?

8. Could this alteration (partially) be explained by the revelations?

9. Do you see any institutional reform as a result of the revelations?

Position of office-holders

10. If any, which office-holders were held accountable as a consequence of the crisis?
11. Did they accept this responsibility in your opinion?
12. Did the crisis influence the position of other office-holders to any extent?
13. Did the media influence this process?

Concluding remarks

14. Is there relevant data or information to either of the cases that you would recommend?
15. Are there comparable cases of cyber crisis, nationally or internationally, that you think should be included in the research?
16. Are there any other people that you could recommend as a respondent for this research?
17. Do you have any questions for me?

Appendix C: Transcripts of interviews

In the appendices that follow, the transcripts of the conducted interviews are included. Note that the interviews are conducted in Dutch, the native tongue of the interviewer and all interviewees.

As agreed upon with the respondents of this thesis, the full transcripts are withhold in the version that is publicly available.

Appendix C.a: Respondent A (04-01-2017)

Full transcript omitted.

Appendix C.b: Respondent B (16-01-2017)

Full transcript omitted.

Appendix C.c: Respondent C (03-02-2017)

Full transcript omitted.

Appendix C.d: Respondent D (10-02-2017)

Full transcript omitted.