Measuring Resilience to DDoS attacks

Expert interviews and a systematic Literature Review on Resilience to DDoS attacks from a Crisis Management perspective

Master thesis submitted to Leiden University
in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE
in Crisis and Security Management

by

Student – M.C.S. Fukkink, s1664832
Thesis supervisor – Dr T. Tropina

Preface

After an intensive period of study, an significant period of my life comes to an end. What began as a joke of a friend of mine, resulted in combining two master studies. If I am passioned about two things at once, why not combine them? And so I did. I will be honest with you: the past one and a half year were the most intense of my whole life and I would not recommend it to anyone, but it was also much fun. The fantastic people around me made this thesis possible, and I would like to thank you all for supporting me.

I want to thank Tatiana Tropina for being the supervisor of this thesis. With your supervision, or rather mentorship, you helped me whenever I had questions or doubts. After every meeting with you, I had an unprecedented amount of energy to make this thesis a success. You have given me exactly the guidance I needed.

Furthermore, I was astonished by the time, and effort people were willing to share with me. It cannot be overstated how important the help of others has been to this research. This research's foundation is based on the contribution of people with busy schedules, who have taken time off to talk to me.

These people were even willing to review the transcripts, provide several documents, and suggest other respondents. I cannot describe in words how grateful I am for that. Therefore, I would like to thank Jelle Niemantsverdriet, Marco van der Kraan, Greig Marshall, Aiko Pras, Gerald Schaapman, Els de Busser, Cristian Hesselman, Roy Kokkelkoren, Stijn Handgraaf, and Andries Reurink for their contribution to this research.

I sincerely hope you enjoy reading the next chapters of my study.

Max Fukkink

Den Haag, January 27, 2021

Abstract

The duration, intensity, and diversity of Distributed-Denial-of-Service (DDoS) attacks are on the rise and due to the advent of the Internet of Things (IoT) will only increase this trend. As the DDoS attacks on the Belastingdienst, the Bunq bank, internet site Tweakers, and internet provider Tweak show, even Dutch teenagers can perform DDoS attacks on vital organisations such as financial and governmental institutions. Therefore, DDoS attacks pose a real treat to Dutch society. Presented in the report of the NCSC (2019), the main issue with DDoS attacks is the lack of resilience measurements.

This research approaches the defence against DDoS attacks from a new perspective. It substantiates the choice to start with resilience instead of security and explains the differences between the two notions. The research extends the resilience matrix of Linkov et al. (2013-b) to offer organisations an holistic view to DDoS mitigation. The matrix did not provide measurable elements and was not designed for DDoS attacks. For this reason, this research consists of expert interviews and a literature study to redesign the matrix. The research finds elements in the different domains and phases and suggests new aspects and adjustments to the resilience matrix.

By rethinking the resilience matrix, this research suggests measurable aspects, interrelations between the aspects, and outcomes for resilience. It becomes evident that measuring resilience requires more emphasis on the planning and preparation phase, a new legal domain, and on splitting the social domain into an internal and external domain.

It also lays out the steps to an overall system resilience and finds that this requires the metrics to involve the interrelationships between the aspects and cells of the matrix, something previous scholars overlooked. In addition, resilience will only be shown during a test or attack. It is up to the organisation to determine in which of the two situations they would prefer to find out. Finally, a resilience measurement will become less valid over time. Therefore, organisations would need to re-evaluate their systems regularly.

This study paves the way for future research. Based on the findings, it is evident that scholars should aim to adjust the selection of interviewees, involve scholars with different backgrounds, take interrelationships into account, add measurements on individual aspects, include weights, and append aspects in the legal, internal, and external domains.

Table of Contents

List of tables and figures

List of abbreviations

CDN – Content Delivery Network

CERT – Computer Emergency Response Team

CTI – Cyber Threat Information

DDoS – Distributed-Denial-of-Service

DMZ – Demilitarized Zone

DNS – Domain Name System

GFR – Gradual Feature Reduction

HSD – The Hague Security Delta

ICT – Information and Communications Technology

IoT – Internet of Things

NAS – National Academy of Sciences

NBIP – Nationale Beheersorganisatie Internet Providers

NCSC – Nationaal Cyber Security Centrum

NCW – Network Centric Warfare

NFV – Network Functions Visualisation

PCA – Principal Component Analysis

SIDN – Stichting Internet Domeinregistratie Nederland

Introduction

On August 16, 2013, DigiD, a tool for identification on governmental websites, was attacked by a Distributed Denial of Service (DDoS) attack disabling people to log in on governmental websites between 08.00 and 16.15 hours (De Volkskrant, 2013). The incident was not the first time a DDoS attack shut down DigiD, and according to a spokesperson of DigiD, it would probably not be the last time either (De Volkskrant, 2013; Van Unen, 2018). In 2018, an 18-year-old boy was being suspected of executing multiple DDoS attacks on de Belastingdienst, the Bunq bank, internet site Tweakers, internet provider Tweak (Verhagen, 2018), and several banks causing their systems to go offline (Paauwe, 2018; Modderkolk, 2018; NCSC, 2019). He wanted to have some fun and show that a teenager could shut down all the Dutch banks (Modderkolk, 2018).

Financial and governmental institutions are vital for Dutch society, and as even teenagers can perform DDoS attacks on those institutions, one could only image what professionals would be able to do. Unfortunately, the duration, intensity, and diversity of DDoS attacks are on the rise (Wang et al., 2018) as well as the strength and frequency (Chadd, 2018). Not all attackers commit their crimes just for fun but also revenge, competition, business rivalry, financial benefits, mischief, flaunting their skills, an intellectual challenge, terrorism, cybercrime, cyber espionage, cyberwarfare, cybersabotage, or political beliefs are motivations (Munnichs, Kouw, & Kool, 2017; Salim, Rathore, & Park, 2019). The attackers are not only children but also governments, enterprises, cybercriminals, cyberterrorists, or hacktivists (McKinsey & Company, 2011). On the dark web, DDoS attacks are even traded as 'DDoS-as-a-service' with sometimes round-the-clock support of helpdesks (Munnichs et al., 2017: 13). Therefore, relatively low-end hackers can undermine the continuity of a business (Hull, 2018) and DDoS attacks pose a real threat (Capgemini, 2017).

In 2018, the National Coordinator for Security and Counterterrorism (NCSC) of the Netherlands registered an increase of 15% in DDoS attacks in the Netherlands compared to 2017 (NCSC, 2019). The arrival of the Internet of Things (IoT) – *'a growing number of devices, including household appliances, wearable, TVs, self-driving cars, and medical equipment connected to the Internet'* – contributed to this increase due to the lack of implemented security measures (Munnichs et al., 2017: 9; EESC, 2018). A 'speed-to-market strategy' rather than a 'security-by-design strategy' enabled the IoT's dangers (World Economics, BCG, & Hewlett Packard Enterprise, 2017: 5). This culpable strategy resulted in many vulnerable devices that

hackers could use to create massive botnets such as the Mirai, Hajime, and Reaper botnets (ISC^{2}NL, 2019). Nowadays, IoT devices pose a real risk (April et al., 2019).

The stakes are higher than ever before, and organisations must understand precisely how to detect and protect themselves from DDoS attacks (Chadd, 2018). Therefore, vital institutions need to prepare for upcoming DDoS attacks. The main issue with DDoS attacks presented in the NCSC report (2019) is the lack of resilience measurements. These measurements would give insights into the efficiency and effectiveness of the implemented measures for resilience (NCSC, 2019). By measuring resilience, policymakers could assess multiple means against DDoS attacks and determine which means would improve a cyber system's resilience the most. This urge for a measurement for resilience results in the following research question: *'What factors could be used to measure the resilience of cyber systems to DDoS attacks?'*

Unfortunately, the current literature is not sufficient in answering this question. Research on measuring resilience led primarily to the resilience matrix of Linkov and colleagues (2013-b), and this matrix is not even specified to DDoS attacks, nor is it able to provide specified measurements. Beyond the academic scope, various consultancy firms also endeavour to offer resilience metrics (Deloitte, 2018; Capgemini, 2017; Hull, 2018; Hoorweg & De Koning, 2015; PwC, 2016; Accenture, 2018; McKinsey & Company, 2011; World Economic Forum et al., 2017). However, besides first impressions on resilience, those companies refer to their paid services for further assistance. The public domain also needs this information and, therefore, this research will build on the cybersecurity resilience matrix proposed in the study of Linkov and colleagues (2013-b).

The aspects of that matrix need to be specified to DDoS attacks and made measurable. Therefore, this exploratory research aims to determine factors for measuring the resilience of computer systems and networks to DDoS attacks. To attain these factors, this research conducts expert interviews and a literature review.

This research proposal will proceed with a theoretical framework. Then, it continues by setting out the research design and concretises the interviews and literature review. The results of the research will be discussed in the subsequent chapter. In that section, this research examines the insights on aspects for the matrix and also suggests to rethink the matrix. The research wraps up with a conclusion and discussion. Finally, the study will indicate where it hopes future research will proceed.

1. Theoretical framework

This section will discuss the theoretical framework for this research. The section provides previous studies and proposes a resilience matrix to measure an organisation's resilience.

1.1 The DDoS attack

During a DDoS attack, a server is bombarded with communication requests so that the server becomes unreachable for others. Such attacks are prevalent today with the ease of access to large numbers of infected machines, collectively called botnets (Wang, Chang, Cheng, Mohaison, 2018). An attacker infects millions of computers worldwide with some malware. Then, the attacker gets access to those computers and launches massive DDoS attacks. During such an attack, many accommodated targets send a request at the victim's site simultaneously, to exhaust the computing or communication resources within a short period (Nagpal, Sharma, Chauhan, Panesar, 2015). The work of Lange and Kettani (2019) examined the mitigation steps for end-users to prevent their devices from becoming part of a botnet and offered insights on botnet evolution, trends and mitigations, and a broad understanding of the issues involved.

Security researchers and industry devoted enormous efforts to understanding DDoS attacks and defending against them (Wang et al., 2018). It is an arms race between the attackers and the defenders (Wang et al., 2018; Munnichs et al., 2017); *'what is regarded as secure today may be obsolete tomorrow'* (Munnichs et al., 2017: 26). The issue remains on how to respond to and mitigate those attacks and determine which requests are legitimate versus legitimate (Kowtko, 2011). Hesselman et al. (2020) identified three challenges for the Domain Name System (DNS) and IoT industries to enable DNS security functions in popular IoT operating systems to combat IoT-powered DDoS attacks. Those challenges are developing a DNS security and transparency library for IoT devices, developing a system to share information on IoT botnets, and proactive and flexible mitigation of IoT-powered DDoS traffic.

According to Chadd (2018), to stand a chance at winning in the cyberwar, organisations should emphasise cybersecurity as they do on any other part of their business. Minutes of downtime or latency significantly impact brand reputation and, ultimately, revenue generation (Newman, 2019). As stated by Wang and colleagues (2018), understanding the current trends in today's DDoS attacks and their attack vectors is a crucial phase in devising effective defences.

While there is much variety between DDoS attacks, one of the most common forms of attack is dual-purpose: using a DDoS and to then plant ransomware, viruses, or malware

(Chadd, 2018). So, DDoS attacks are no longer only designed to cause only a denial-of-service or take websites down, but a shorter stealthy attack can now act like a 'Trojan horse' to mask other malicious activity, including network infiltration and data theft (Newman, 2019). Moreover, short DDoS attacks allow cybercriminals to test for vulnerabilities within a network (Newman, 2019). In such cases, those attacks serve as a 'smokescreen' for other malicious activity (EESC, 2018: 23). Unfortunately, a large-scale view of today's DDoS attacks is missing in the literature (Wang et al., 2018). This shortcoming complicates the understanding of the trends of DDoS attacks, their attack vectors, and the devising of effective defences, including the development of a comprehensive resilience measurement system.

1.2 Computer systems and security

Researchers already have made a tremendous effort to indicate the security of computer and information systems. In the field of computer science, the term information security first emerged to describe activities relating to the protection of information and information infrastructure assets against the risks of loss, misuse, disclosure, or damage (Van den Berg et al., 2014). In this notion, the CIA trait consisting of the values confidentiality, integrity, and accountability are key (Van den Berg et al., 2014). Later, scholars extended information security with terms like authenticity, non-repudiation, and accountability to make it become cybersecurity (Van den Berg et al., 2014). In broader terms, security connotes the objective state of being without or protected from threats (Zedner, 2003). In his paper, Baldwin (1997: 13) uses the notion of *'a low probability of damage to acquired values'*. Subsequently, he argues to question: Security for whom, for which values, how much security, from what threats, by what means, at what cost, and in what time? Those questions construct the components for security.

With security, the terms threat, vulnerability, and risk come along. Jones (2005) points out that the profession did not adopt standard definitions for those. He defines those concepts as a threat - *'anything that is capable of acting against an asset in a manner that can result in harm'*, a vulnerability - *'a weakness that may be exploited'*, and a risk - *'the probable frequency and probable magnitude of future loss'* (Jones, 2005: 5). Thus, security is inevitably connected to risk.

Then, Jones (2005: 18) decomposes risk into 'Loss Event Frequency' and 'Probable Loss Magnitude'. For Loss Event Frequency, he uses 'the probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset'. And, he describes Probable Loss

Magnitude as containing the factors that drive loss magnitude when events occur. The researcher divides the former into 'Threat Event Frequency' and 'Vulnerability' (Jones, 2005: 18). Threat Event Frequency means *'the probable frequency, within a given timeframe, that a threat agent will act against an asset'* (Jones, 2005: 18). Thus, security depends on the risk, which is, in turn, partly determined by the attacker.

1.3 Risk Assessment and a catch

Previous research has made an effort to indicate the security of cyber systems with risk assessment methods. Jones (2005) introduced the Factor Analysis of Information Risk. Norman and Neil (2012) use a causal model and Bayesian networks. Cox (2009) considers Game Theory for risk analysis. Rosenquist (2009) gained notoriety with the Threat Agent Risk Assessment, which distils the number of possible attacks into those most likely to occur. Noroozian, Ciere, Korczynski, Tajalizadehkhoob, and Van Eeten (2017) presented a model to estimate security performance and also suggested to aggregate information from different models by using, for example, the Borda count method. Pieters (2009) made an effort to create a model defining a system's weakest link. Labunets (2017) underlined the difference between the tabular industry methods such as ISO 270001, NIST 800-30, SESAR SecRAM, and SREP and academic methods with graphical modelling notations such as SI* Secure, Tropos, ISSRM, and CORAS. Another standardised assessment methodology is the Common Vulnerability Scoring System (CVSS) (Mell, Scarfone, & Romanosky, 2007; Collier et al., 2014). Also, Sanders (2014) categorised current security metrics into three categories:

- Organisational security metrics: those used to describe and track how effectively organisational programs and processes achieve cybersecurity, e.g. the Guide for Assessing the Security Controls in Federal Information Systems and Organisations and the Systems Security Engineering Capability Maturity Model.
- Technical security metrics: those indicate the level of security of a specific system, e.g. the Common Methodology for Information Technology Security Evaluation (CEM) and the Common Vulnerabilities and Exposures list
- Operational security metrics: those describe and manage the risks on an operational environment and include measures of operational readiness or security postures, measures used in risk management, metrics describing the threat environment, metrics supporting incident response and vulnerability management.

Now here is the catch: security frameworks make organisations indicate how likely it is a particular classification of attackers conduct an attack on the organisation. However, it is challenging to provide these indications. Therefore, it is also hard to offer valid indications on the probabilities of attackers attacking the organisation's systems. This fact could seriously undermine the validity and effectiveness of security models. Why would an organisation approach DDoS attacks from this angle despite having so little information on attackers and the likelihood of their behaviour despite having minimal information on this?

1.4 Cyber Resilience

This research would like to approach the problem from another angle and to suggest to use resilience instead of security. Defined by the Oxford dictionary, resilience is *'the ability of people or things to feel better quickly after something unpleasant, such as shock, injury, etc.'* or *'the ability of a substance to return to its original shape after it has been bent, stretched, or pressed'* ("Resilience," n.d.). Merriam-Webster defines resilience as *'the capability of a strained body to recover its size and shape after deformation caused especially by compressive stress'* and *'an ability to recover from or easily adjust to misfortune or change'* ("Resilience," n.d.). Linkov and colleagues (2013-b) use the last definition of resilience in their research. Those researchers also underline the difference between resilience and risk, although current concepts and methods sometimes conflate those concepts. Their study uses the definition the *'ability to withstand and recover quickly from unknown and known threat'* for resilience and the *'product of the likelihood of an adverse event and the magnitude of the resulting damage'* for risk (Linkov et al., 2013-b: 472). They advocate for resilience systems that utilise concepts distinct from risk assessment.

Taking an approach that differs from the status quo would enable organisations to consider DDoS and cyber-attacks in general without reasoning in terms of chances, odds, possibilities, and probabilities. These concepts are hard to grasp, challenging to discuss with laypeople, and require much knowledge about the adversaries. With the concept of resilience, organisations can approach the DDoS problem from their systems, which they presumably know much more about. Besides, organisations are primarily interested in whether their systems can recover from an attack and how well and fast it can achieve this.

Although resilience earned its significance among scientists, engineer, and planners in a variety of socioecological fields and there have been calls for U.S. federal agencies to implement resilience, the implementation of resilience in cybersecurity is rather limited.

First efforts in providing resilience metrics for cyber systems are established in the literature. The National Academy of Sciences (NAS) reported on 'disaster resilience' as a system's ability to perform four functions concerning the following events: planning and preparation, absorption, recovery, and adaption (The U.S. National Academy of Sciences, 2012).

In the first stage, planning and preparing, policymakers lay the foundation to keep services available and assets functioning during a disruptive event (malfunction or attack). Secondly, absorption is concerned with maintaining the most critical asset function and service availability while repelling or isolating the disruption. Thirdly, the recovery stage restores all asset function and service availability to their pre-event functionality. Finally, the fourth stage, adaptation, focusses on using knowledge from the event, alter protocol, the configuration of the system, personnel training, or other aspects to become more resilient (Linkov et al., 2013-a).

After this phase, the model cycles back to the plan and preparation phase and starts moves to the absorption phase when another adverse event happens (Linkov et al., 2013-a). Thus, the model makes a cyclical movement. In a paper by Bodeau, Graubart, Picciotto, McQuaid (2011) of MITRE, the writers pointed out resiliency goals: anticipate, withstand, recover, and evolve. The descriptions of these goals are very similar to the phases of Linkov et al. (2013-b).

Linkov and colleagues (2013-a) pointed to military scholars who proposed the doctrine of Network Centric Warfare (NCW), which focuses on creating shared situational awareness and decentralised decision-making by distributing information across networks operating in physical, information, cognitive, and social domains. The paper of Eisenberg et al. (2014: 5) provides a general description of the domains:

- Physical: *'the engineering capabilities of infrastructure or devices, efficiencies, and network structures. This includes all data collection equipment and measurable real-life system components'*;
- Information: *'the usage of what we measure and know about the physical domain, including data use, transfer, analysis, and storage'*;
- Cognitive: *'human processes, i.e., translating, sharing, and acting upon knowledge to make, communicate, and implement decisions throughout the system'*; and
- Social: *'interactions and entities that influence how decisions are made, including government regulations, religions, cultures, and languages.'*

Then, Linkov et al. (2013-b) applied these domains to computer and information systems. Firstly, the physical domain includes sensors, facilities, equipment, system states and capabilities (Linkov et al., 2013-a). Secondly, the information domain includes creating, manipulating, and storing data (Linkov et al., 2013-a). Thirdly, the cognitive domain encapsulates understanding, mental models, preconceptions, biases, and values (Linkov et al., 2013-a). And the final domain, the social domain, includes interaction, collaboration, and self-synchronisation between individuals and entities (Linkov et al., 2013-a). After this phase the

These domains determine the characteristics of the cyber system. *'The resilience of a cyber system is dependent on the effective functioning of all aspects of an organisation throughout the event management cycle in the four identified domains'* (Linkov et al., 2013-b: 475). To illustrate the influences of the different domains, a small online store has a whole other cyber system than a governmental tool such as DigiD. If DigiD is targeted, it has different physical attributes, ways of handling data, understandings, and involved actors based on the four domains compared to the system of an online store. Thus, because of their different characteristics, they have also other vulnerabilities.

In their subsequent paper, Linkov and colleagues (2013-b) tailor the resilience matrix framework to cyber systems. This matrix is illustrated in the table of Appendix B. The metrics in this matrix are based on quantitative and qualitative data, which are evaluated by technical experts (Linkov et al., 2013-b). For each factor in the matrix the evaluation will be based on the question: *"How is the system's ability to [plan/prepare for, absorb, recover from, adapt to] a cyber disruption implemented in the [physical, information, cognitive, social] domain?"* (Linkov et al., 2013-b: 473). For example, suppose a better understanding of the system's creation, manipulation, and data storage in the recovering phase is needed. In that case, an expert's question becomes: 'How is the system's ability to recover from a cyber disruption implemented in the information domain?'

1.5 A conceptual model and redesigning the matrix

Figure 1 illustrates the conceptual model of resilience derived from Linkov and colleagues (2013-b). They divide a cyber system into the four specified domains, the physical domain, the information domain, the cognitive domain, and the social domain. From the matrix of Linkov and colleagues (2013-b), it is also possible to derive factors for the resilience of cyber systems. For example, in the physical domain and during the planning and preparing phase, Linkov and

colleagues emphasise, among other things, to implement controls/sensors for critical assets. Those are not factors but imperatives. However, this research will not exclude them as possible factors for resilience against DDoS attacks but rather restate the essence of those aspects.

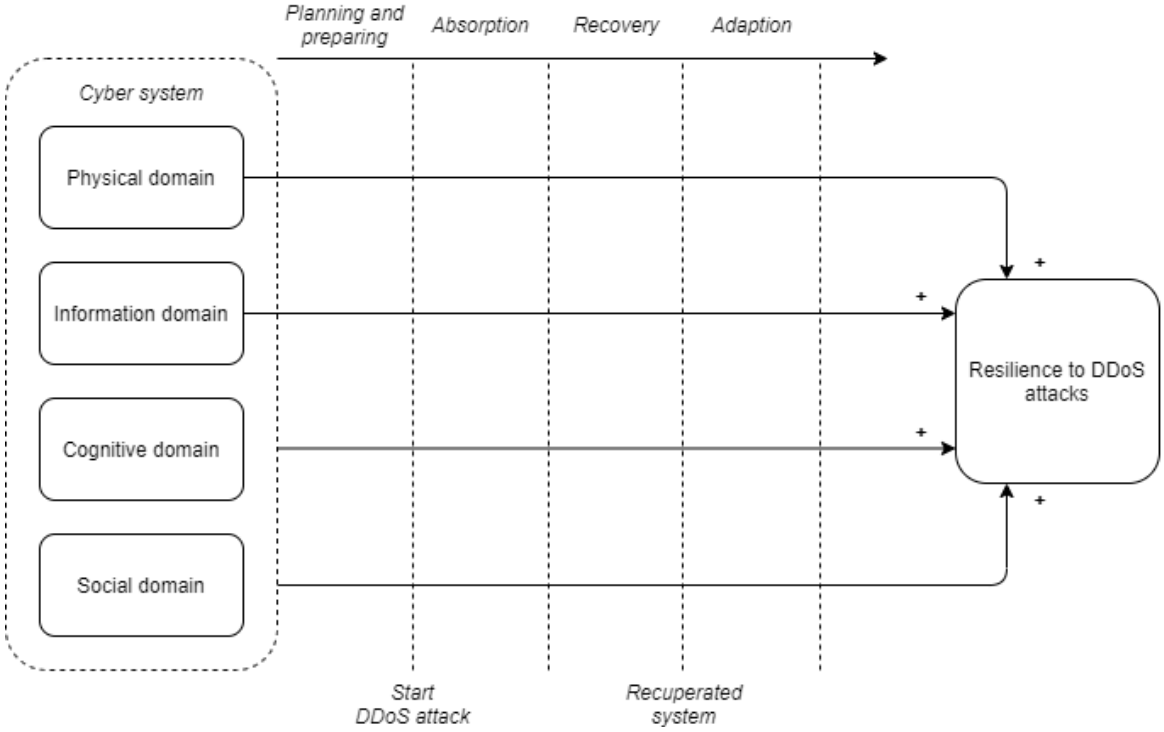

Figure 1: Conceptual model of a cyber system's resilience to DDoS attacks

The matrix of Linkov and colleagues (2013-b) suggests that implementations of the matrix factors result in a cyber system's resilience. Therefore, this research is expected to further substantiate improved implemented factors in the different domains over the different phases to enhance the resilience to DDoS attacks. The term improved factors is used for factors that mitigate more DDoS attacks or more up-to-date DDoS attacks than outdated implementations of factors. The matrix also suggests that it is possible to differentiate between phases around a DDoS attack, such as the planning and preparation, absorption, recovery, and adaption phase.

In 2020, Marchese, Jin, Fox-Lent, and Linkov (2020) identified and organised various functions of smart water systems and applied the model of Linkov and colleagues (2013-b). Moreover, Wood, Wells, Rice and Linkov (2019) used the matrix to quantify and map resilience within a large organisation. It shows the model's flexibility in that the model lends itself to be applied to specific matters.

Researchers also have applied the resilience matrix to the coastal community resilience at Rockaway Peninsula, New York (Fox-Lent, Bates, & Linkov, 2015); disaster-induced population displacement (Rand, Kurth, Fleming, & Linkov, 2020); Urban Resilience Planning

(Fox-Lent & Linkov, 2018); electrical engineering (Zussblatt et al., 2017); the U.S. building industry (Kurth, Keenan, Sasani, & Linkov, 2018); and value chains (Linkov et al., 2020). Moreover, DiMase, Collier, Heffner, and Linkov (2015) pointed to the challenges of cyber-physical security systems and argued for a systems-based view that interweaves the various areas of concern in a construct that is robust and resilient.

Specifying the matrix of Linkov and colleagues (2013-b) and the resulting conceptual model to a framework for resilience to DDoS attacks will enable system owners to measure their system's resilience. Therefore, this paper aims to provide this specification to contribute a measurable resilience to DDoS attacks.

2. Research design

This chapter discusses the methodology of the research. The study involved a mixed-methods approach consisting of semi-structured expert interviews and a systematic literature review. This section provides a description of the interviews and the literature review.

2.1 Interviews

This research conducted multiple interviews with professionals in the field. At this point, Linkov and colleagues' matrix (2013-b) provided factors of resilience, but those are not specified to DDoS attacks and somewhat vague. For example, *'implement controls/sensors for critical assets'* does not define control/sensors and when an asset becomes critical, thus, does not provide policy-makers with a measurement. So, a more in-depth understanding of the concepts is needed. In doing so, this research will inductively expand the current theory. Therefore, a qualitative research method was needed.

Cybersecurity experts in the field must have some guidelines on how to prepare cyber systems for DDoS attacks. After all, the affected organisations presented in the introduction recovered after downtime from a DDoS attack (De Volkskrant, 2013; Van Unen, 2018; Verhagen, 2018; Modderkolk, 2018). As this research will be exploring the views and experiences of individuals participants, interviews are the right research method.

2.1.1 Selection of interviewees

The selection of interviewees is inspired by the approach and techniques of previous research. For example, the study of Munnichs and colleagues of the Rathenau Institute (2017) managed to conduct interviews and organised workshops with Europol, ENISA, Dutch Ministry of Defence, NCSC, Dutch internet providers, Dutch banks, a Dutch cybersecurity company, and multiple Universities.

This research included eight organisations and his subsection will discuss those organisations. The first two organisations were the NBIP and SIDN. The NBIP, a non-profit organisation that helps internet providers comply with legal requirements and ensures adequate coverage of security risks, in collaboration with the SIDN, a foundation that manages the register of domain names for the top-level domain .nl, already conducted quantitative research on DDoS attacks (NBIP, 2018). Their study involved 237 DDoS attacks between July 1, 2017, and June 30, 2018.

As the introduction illustrated, Dutch banks are one of the victims of DDoS attacks. Those organisations have dealt with such attacks in the past. Therefore, this research included employees of the Rabobank and ABN AMRO.

Moreover, the introduction also addressed consultancy companies' services on DDoS mitigation. To cover the unique perspective on advising side of the problem, this research involved an employee of Deloitte.

Other involved respondents were academia from the University of Twente and Leiden University. Especially researchers from Twente already provided many studies on the mitigation of DDoS attacks. This research aimed to include their visions and perspectives.

Finally, an employee of the NCSC of the Netherlands (NCSC-NL) was also a respondent of this research. That organisation understands vulnerabilities and threats; connects parties, knowledge, and information; and prevents social damage and limit threats (NCSC, n.d.-a). Moreover, it is also an essential party in the coordination during major ICT crises and the Computer Emergency Response Team (CERT) for the Dutch central government (HSD, n.d.). Unfortunately, this interview could not be involved as the approval for this was not received.
Table 2 presents this selection including the name of the organisation, a short description of the organisation, the interview's date, the interview's duration, the respondent's name, and the respondent's position.

Before starting the period of interviewing, this research included a test interview with a befriended Computer Science student Andries Reurink. This test allowed to make potential adjustments to the interview questions, test the recording equipment and the video call software, improve the lighting in the interviewer's room, and it showed that the interview would take approximately one hour and fifteen minutes.

Table 2 also shows that the research conducted the interviews in a period of four months. The interviews took between one and three hours but on average, one hour and 30 minutes. Due to the worldwide pandemic, this research did not involve any interviews in person but with video call software such as Zoom and Microsoft Teams. To make sure no recordings would be lost, the video call software, another laptop, and a mobile phone recorded the interviews. This turned out to have been a great addition because some devices failed in cases or the recorded volume was too low to make a suitable transcript.

After the interview, the respondents had the opportunity to view the transcript, make adjustments, and possibly delete confidential elements. In general, the respondents used this opportunity to make improvements and to correct certain statements and provide additional

explanations. The result section of this research refers to the surnames of the respondents and puts them between round brackets. For example, the section would refer to a result based on the interview with Jelle Niemantsverdriet as (Niemantsverdriet). Appendix A presents the interviews' transcripts.

Then, the research analysed the transcripts with Atlas.ti[1]. This software enables qualitative data analysis and research. This research primarily used the combinations of phases and domains as codes to structure the interviewees' responses according to the resilience matrix. The research also included codes like 'suggestions' and 'interrelationships' to cover responses that did not fit within the matrix.

Table 2: Final selection of organisations and respondents

organisation	*description*	*date*	*duration*	*respondent*	*function*
Deloitte	Consultancy company	April 21, 2020	1.5 hrs	Jelle Niemantsverdriet	Director Cyber Risk Services
Rabobank	Bank	May 7, 2020	1.25 hrs	Marco van der Kraan	Security specialist
ABN AMRO	Bank	May 8, 2020	1.75 hrs	Greig Marshall	Product owner
University of Twente	University	May 14, 2020	1.25 hrs	Aiko Pras	Professor in Internet Security
NCSC-NL*	Cyber information hub and CERT for the Dutch central government	May 27, 2020	3 hrs	Stijn Handgraaf	Security specialist
NBIP	Independent, non-profit organization for Internet and VoIP service providers	June 16, 2020	1.25 hrs	Gerald Schaapman	Co-owner SVSnet
University Leiden	University	July 6, 2020	1 hr	Els de Busser	Assistant professor and program director
SIDN	Registry top level domain .nl	August 21, 2020	1.5 hrs	Cristian Hesselman	Director of SIDN Labs

*: permission to use this interview was not received in time

2.1.2 Operationalisation of the interviews

The interviews had starting and followed-up questions based on prompts. This research consisted of semi-structured interviews to guide interviewees but keeping a level of flexibility. The interviewees were first introduced to the research's aim and the Linkov and colleagues' (2013-b) matrix. Therefore, the interviewer started by explaining the different domains and phases of the matrix. Then, the interviewer questioned the respondent's opinion on the matrix.

After that, the interviewer asked about the respondent's view on resilience factors per domain and per phase. The formulation of Linkov and colleagues (2013-b) discussed earlier, *'How is the system's ability to [plan/prepare for, absorb, recover from, adapt to] a cyber disruption implemented in the [physical, information, cognitive, social] domain?'* (Linkov et al., 2013-b: 473), was reformulated to 'From your point of view, what factors indicate *'the*

[1] Atlas.ti: https://atlasti.com/

system's ability to [plan/prepare for, absorb, recover from, adapt to] a DDoS attack implemented in the [physical, information, cognitive, social] domain?'. Thus, the question is specified to DDoS attacks and is now questioning which factors will indicate this. Also, the questions will follow the phases and domains of the matrix. Thus, the questioning started with discussing the planning and preparing phase in the physical domain, discussed the absorption phase also in the physical domain, and continued as such. For example, the first question of those was: 'From your perspective, what factors indicate the system's ability to *plan/prepare* for a DDoS attack implemented in the *physical domain*?'

Besides that, this research constructed the prompts for the specific questions based on Linkov and colleagues' matrix factors. To illustrate, the prompts for the just constructed question on the physical domain in the planning and preparing phase are based on implementing controls/sensors for critical assets, implement controls/sensors for critical services, assessment of network structure and interconnection to system components and the environment, redundancy of critical physical infrastructure, and redundancy of data physically or logically separated from the network (Appendix B). Those indications are reformulated to factors resulting in controls/sensors for critical assets, controls/sensors for critical services, network structure and interconnection, redundancy of critical physical infrastructure and data. The interviews used those as prompts in the interviews. Continuing with this construction of questions and prompts over the whole matrix created the interviews' structure, and is presented in table 3 (Appendix C).

2.2 Systematic literature review

The research of Dijkman, Sprenkels, Peeters, and Janssen (2015) redesigned the business model framework for Internet of Things applications. Their study included semi-structured interviews and followed the framework's structure to guide the respondents through the questions. Inspired by their research, this study also combines expert interviews with a literature study to substantiate the interviews' findings further. Another example is the study of Harrison (2015). That researcher also conducted a literature study and interviews on cyber-bullying. Finally, Zheng and Julien (2015) analysed the challenges of verification and validation in cyber-physical systems. Their research also included a literature review and interviews.

The main difference between the studies of Dijkman et al. (2015), Harrison (2015), and Zheng and Julien (2015) and this research is that they conducted the literature study first and

then the interviews, while this study did that vice versa. The study of Sayagh, Kerzazi, Adams, and Petrillo (2020) also performed the interviews before the literature review. Those researchers came to nine essential configuration engineering activities and, with the literature review, put those findings in perspective, identified overlooked practices, and guided practitioners to published approaches and solutions.

This research also aimed to substantiate the interviews' findings further, identify overlooked aspects, and guide experts to published solutions. Therefore, it consisted of systematic literature after the interviews. The work of Webster and Watson (2002), Levy and Ellis (2006), and Wee and Banister (2016) offered the methodology for the review. They approached the systematic review with three steps. Webster and Watson first focussed on research from leading journals.

After that, the researchers suggested to review the references of those articles and search for studies that cite the work found in the initial step. Those researchers spoke of moving forwards and backwards. Levy and Ellis call these steps the keyword search, the backward search, and the forward search. Although they come down to the same thing, Wee and Banister (2016) used the terms backward and forward snowballing. This research followed the approaches of Webster and Watson (2002), Levy and Ellis (2006), and Wee and Banister (2016). The next section explains exactly how this research applied that method of a systematic literature review.

2.2.1 Operationalisation of the systematic literature review

The keyword search of this research consisted of four different keyword combinations on IEEE Explore and Scopus. The hits were sorted on relevance and this research studied a maximum of fifty studies per search. Table 4 indicates the results of each search in hits, studied articles, the number of relevant articles, and the number of new studies.

Table 4: Keyword search results

Source	*Keyword combination*	*Hits*	*Studied*	*Relevant*	*New*	*Date*
Scopus	DDoS AND holistic AND (defen* OR mitigat*)	6	6	2	2	28/01/2021
	DDoS AND social OR legal	264	50	2	2	28/01/2021
	DDoS AND (legal OR law)	124	50	9	9	28/01/2021
	DDoS AND crisis AND management	6	6	2	2	29/01/2021
Xplore	DDoS AND holistic AND (defen* OR mitigat*)	2	2	1	0	29/01/2021
	DDoS AND (social OR legal)	79	50	9	5	29/01/2021
	DDoS AND (legal OR law)	57	50	6	1	29/01/2021
	DDoS AND crisis AND management	0	0	0	0	29/01/2021

For the back and forward search, this research considered the most relevant article from the keyword searches and the paper of Linkov et al. (2013-b). Table 5 shows the results of these search steps.

Table 5: Backward and Forward search results

	Backward					*Forward*				
Article	*Citations*	*Studied*	*Relevant*	*New*	*Date*	*Citations*	*Studied*	*Relevant*	*New*	*Date*
Linkov et al. (2013-b)	20	20	0	0	29/01/2021	187	50	7	6	29/01/2021
Backman (2020)	44	44	2	2	29/01/2021	0	0	0	0	29/01/2021

The most significant decision was to avoid technical literature. It is tempting to approach cybersecurity from a computer science perspective. However, this research aimed to scope beyond this approach. Whenever possible, this research stayed on the surface of this discipline and involved crisis and security management. Technical papers have certainly come along and are, therefore, mentioned in the result section. Nevertheless, this research attempted to generalise technical factors and indicate the options available. If there is a specific curiosity in particular methods and techniques, this research gladly refers to the relevant scholars.

In addition to the literature provided from the collection method described above, this research also included reading suggestions of the interviews' respondents and reports from email subscriptions of involved actors such as CDN service providers.

3. Analysis

This section combines the insights of the interviews and literature review. It follows the structure of the matrix and interviews discussing the phases for each domain subsequently. This section starts with the physical domain elaborating on its phases and then moves on to the information domain until the social domain. In each domain's fifth subsection, the research provides conclusions on the domain. Those sections discuss striking findings, a summary, and an overview of the results of the domain.

3.1 The Physical domain

The physical domain describes the 'physical resources and the capabilities and the design of those resources' (Linkov et al., 2013-b: 473). The next subchapters represent the phases of this domain subsequently.

3.1.1 Planning/preparation phase in the physical domain

In this phase within the physical domain, Linkov and colleagues (2013-b) determined the foundation to keep services available and assets functioning during a disruptive event. Those researchers (2013-b: 474) underline five aspects to be considered: *'implement controls/sensors for critical assets'*, *'implement controls/sensors for critical services'*, *'assessment of network structure and interconnection to system components and environment'*, *'redundancy of critical physical infrastructure'*, and *'redundancy of data physically separated from the network'*. The respondents argued about this phase. They suggested a Mapping on the network structure, Mitigation systems, Detection systems, and Separation of the network.

The first aspect is a mapping of the network structure. Four respondents specifically advocated mapping the computer system's technological structure (Niemantsverdriet, Van der Kraan, De Busser, and Marshall). None of the respondents argued against the mapping of the system. Van der Kraan questioned: *'How are your network and your internet connection built up?'* The cybersecurity company Fox-IT also argued to identify information assets (Fox-IT). According to the company, it will help understand what needs to be protected, where it is located, and any classification handling requirements or regulatory obligations.

Defenders against DDoS attacks can understand the computer network with network mapping. Defenders can draw a map or use simple software to visualize their network. With the network the respondents meant the entire chain: *'From internet line, routers, switches, firewalls, load balancers up to and including the web servers; All components in that chain*

must be resilient enough to deal with sudden session loss or session increase.' said Van der Kraan. Marshall also included: the network structure, interconnections, the number of lines the organisation has, and the number of internet providers the organisation has. The respondents suggested that an organisation with a map will be more resilient than one without a map. The reason for this lays in the possibility to analyse the network.

Secondly, the respondents argued in favour of mitigation systems. Most respondents argued about intervening by adding extra capacity, diverting, or filtering malicious traffic (Niemantsverdriet, Van der Kraan, Schaapman, Marshall, Pras, and Hesselman). More specifically, Niemantsverdriet talked about adding extra capacity; Van der Kraan about Demilitarized Zone (DMZ), firewalls, and redundant assets; Pras and Hesselman about Anycast. This research will not discuss those measures in full detail here. However, it is critical to note that different DDoS attacks require different measures to mitigate them; also, the service of the organisation requires different mitigating measures.

A specific method is NFV/SDN-based mitigation. Network Functions Visualisation (NFV) deploys security functions as software instead of hardware, and virtualised network functions may run on one or more virtual machines (Alharbi et al., 2017). This method does not rely on customised hardware appliances, and resources could be shared with other network functions (Alharbi et al., 2017). The research of Alharbi et al. discussed the different detection and mitigation methods, and designed a framework that leverages NFV and edge computing for DDoS mitigation.

Moreover, most respondents highly doubted whether organisations are even capable of mitigating DDoS attacks themselves nowadays (Niemantsverdriet, Pras, Marshall, and Hesselman). In Marshall's words, the preparation phase includes looking at yourself and saying: *'Can I protect myself? If you say yes, you are either a large tech company or a liar.'* Pras specifically talked about the size of the DDoS attack: *'At fifty Gigabit, there are only very few parties that can withstand such an attack. So, you need help with that. You can hardly get a Gigabit yourself unless you know how to filter properly.'* Almost all respondents pointed at different scrubbing services or content delivery network (CDN) services such as the NaWas, Akamai, Cloudflare, and Fastly (Niemantsverdriet, Van der Kraan, Schaapman, Marshall, Pras, Hesselman; Akamai, n.d.-a). The study of You et al. (2020) also pointed to the economic benefits of outsourcing part of the traffic scrubbing.

The business of such companies is based on the limitation of security hardware capacities (Alharbi, Aljuhani, Hang Liu, 2017). The customer needs to redirect its incoming

traffic to the remote DDoS protection service, to the so-called Scrubbing Centers (You, Jiao, Li, & Zhou, 2020). There, the filtering and mitigation take place, and only filtered traffic returns to the organisation (Alharbi et al., 2017).

Although those companies impact the resilience, this research considers this aspect in the social domain of Linkov and colleagues (2013-b) and, therefore, the corresponding chapter will discuss those services. There is interference between the physical and social domain here. For example, an organisation could mitigate the smaller DDoS attacks themselves and leave the more significant attacks to specialised companies. The organisation will consider their protection measures in the physical domain and the other companies' services in the social domain.

Furthermore, the respondents argued in favour of redundancy (Niemantsverdriet, Van der Kraan, De Busser, and Pras). Linkov and colleagues (2013-b) also mention this as a separate aspect, but this research considers it a part of mitigation systems. Because we focus on the resilience to DDoS attacks, redundant assets mean the capacity to scale up to high volumes of data traffic. An organisation uses this extra capacity to absorb and, thus, mitigate a DDoS attack.

Thirdly, to mitigate a DDoS attack, an organisation would first need to detect an attack. Almost all respondents pointed out the influence of detection capacity for resilience (Niemantsverdriet, Van der Kraan, Schaapman, Marshall, and Hesselman).

The study of Backman (2020) analysed the cyber crises of Estonia and the UK in 2007 and 2017, respectively. The researcher applied the framework of Boin et al. (2005, 2017) to operationalise the crisis management task domains. The current research will do the same and adds different tasks in the corresponding phases and domains. The task of detection is worth mentioning here as it involves discovering and unfolding or emerging crisis events and collecting data about it (Boin et al., 2017; Backman, 2020).

The study of Cavusoglu, Mishra, & Raghunathan (2004) differentiates between two detection systems: signature-based and anomaly detection systems. The signature-based detection looks for attacks that match a predefined pattern. For example, the device could look at the header of data packages. This header is placed in front of the body or payload of a data package, describes the payload, and provides information on data handling. It could contain essential information on whether the package is malicious. To illustrate, a device could identify a package coming from a known malicious source based on the information in the header because of similarities with a previous DDoS attack.

The second type of detection is also applicable to DDoS. The detection devices identify abnormal behaviour using a 'normal' activity profile (Cavusoglu, Mishra, & Raghunathan, 2004). For this second type of detection, defenders need to gather information about the usual traffic that comes to their network. This research discusses the difference between usual and unusual traffic more thoroughly in the cognitive domain. For this domain, it is crucial to understand that there are multiple approaches to detecting DDoS attacks and organisations need different types of detection to catch different types of DDoS.

Moreover, Machine Learning has promising outcomes in detecting DDoS attacks (Das, Venugopal, & Shiva, 2020). The study of Das, Venugopal, and Shiva (2020) pointed to other work on supervised, semi-supervised, and unsupervised methods for DDoS detection. In the same research, they addressed the combination of supervised and unsupervised Machine Learning to detect anomalies, Neural Network and SVM for supervised modelling, KNN for unsupervised modelling, and Principal Component Analysis (PCA) and Gradual Feature Reduction (GFR) for feature selection with NSL-KDD dataset.

The most common DDoS attacks are based on the OSI model's network and application layer (Van der Kraan and Schaapman). The first one is relatively easy to detect. Schaapman provided an example: an organisation can handle a maximum of 10 Gigabits, and when an attack of 20 Gigabits comes in, then the connection is overloaded and shuts down. This incident is immediately visible. Pras also explained this type of attack. The second type is harder to detect (Schaapman). Those attacks are based on the application layer and do not even require a large traffic volume. During such an attack, the malicious traffic let the victim's server wait for an extended period or makes it execute very computationally intensive tasks. To detect that kind of attack, an organisation will need 'smarter' devices. Those look independently at various protocols and headers to come to mitigation rules (Schaapman).

An organisation could also decide to implement multiple detection devices to detect comparable DDoS attacks but with different approaches. If one method turns out to be insufficient in detecting a DDoS attack, other devices will still indicate an attack. This research, therefore, expects that more implemented devices with different approaches will result in more resilience.

The fourth aspect is separation, as an organisation does not want to run everything through one zone. Two respondents talked about this aspect (Van der Kraan, De Busser). For example, an organisation can decide to direct inbound customer traffic different from outgoing traffic. If an organisation does not do this, and an attack comes via the incoming customer

traffic, which is most sensitive for attacks, no more traffic can enter or exit (Van der Kraan). When an attack happens, separation makes it possible only a part of the network is lost.

3.1.2 Absorption phase in the physical domain

During the absorption phase, we need to keep the most critical assets functional and services available while repelling or isolating the disruption (Linkov et al., 2013-b). In this phase, Linkov and colleagues (2013-b: 474) provided aspects to consider. Those are *'signal the compromise of assets or services', 'use redundant assets to continue service'*, and *'dedicate cyber resources to defend against attack'*.

The respondents of this research proposed aspects comparable to the preparation phase. After all, in the previous phase, an organisation has planned what will happen during an attack. The aspects are Working mitigation and detection systems, Sufficient separation, and a Tracker of the response time.

During this phase, the resilience is primarily whether the implementations are doing the things they are supposed to do. Niemantsverdriet argued: 'Can you detect it when something like this happens?' 'Can you scale extra capacity or send some of the traffic elsewhere?' Thus, comparable to the statements in the previous section, the organisation wants to make sure the mitigation systems (Niemantsverdriet, Van der Kraan, Schaapman, Marshall, Pras, and Hesselman), as well as the detection systems (Niemantsverdriet, Van der Kraan, Schaapman, Marshall, and Hesselman) are doing their jobs during an attack. Those systems ought to detect or mitigate specific attacks.

When the system is absorbing an attack, this is also when it becomes clear whether the defenders implemented the separation correctly. If the system is not set up correctly in terms of separation, the attack will shut down more internet pathways than planned (Van der Kraan).

In general, the system mitigates a DDoS attack or not and detects a DDoS attack, or it does not detect it. When an attack is set in motion webservers will be overloading, crashing, popping out of its memory, or making a reboot and mail systems can come to a standstill. In such a case, a detection system that registers the attack ought to contribute more to the system's resilience than a detection system which does not. Moreover, the detection systems that extract more relevant information about the DDoS attack contribute more to resilience. This research considers relevant information as all the information needed to mitigate the attack and required for possible partners to prepare for a comparable attack.

Finally, during the absorption phase, an organisation wants to detect an attack as fast as possible. It is essential to keep the time between a DDoS attack and mitigation finite and short (Akamai, n.d.-b). It is also here the organisation will keep track of the Response time (De Busser, Marshall, Hesselman).

3.1.3 Recovery phase in the physical domain

The victims restore all of the functionality and service availability to the system's pre-attack functionality in the recovery phase (Linkov et al., 2013-b). In their paper, Linkov and colleagues (2013-b: 474) describe four aspects in this phase of the model: *'investigate and repair malfunctioning control or sensors'*, *'assess service/asset damage'*, *'assess distance to functional recovery'*, and *'safely dispose of irreparable assets'*. The respondents of this research argued in terms of Assessment of service/asset damage, Reparation or replacement of damaged assets, Reparation or replacement of malfunctioning detection or mitigation systems, Reparation or replacement of malfunctioning mitigation devices, a System to measure the recovery time, and the Required functionality.

Almost in all cases, the system recovers immediately after a DDoS attack (Van der Kraan). Then, the systems are rebooted and brought to their original state (Schaapman and Pras). Some respondents told about two exceptional cases which happened a long time ago. A DDoS attack damaged assets that had to be replaced (Van der Kraan, Schaapman). Although it is improbable, this research will not exclude the possibility of an attack damaging the system as it could potentially happen. Therefore, this research includes assessing service/asset damage and reparation or replacement of damaged assets, although this will almost always be a matter of rebooting the system.

Secondly, two respondents then argued about the main goal of the recovery phase is to gather information about the attack (Niemantsverdriet, Van der Kraan, and Marshall). Although the information domain will go deeper into this subject, the information will come from the detection devices in the physical domain. If any malfunctioning controls or sensors, an organisation would like to fix those devices (De Busser). None of the respondents specifically mentioned the need for this step but considering the influence of detection systems and mitigation systems on resilience it follows logically to repair those devices that do not register a DDoS attack. For this reason, this research will include the reparation or replacement of malfunctioning detection devices and reparation or replacement of malfunctioning mitigation devices.

The third and fourth aspects are a system to measure the recovery time and a determination of the required functionality. An organisation needs to get its services running again as fast as possible. The organisation with a higher resilience would have a shorter recovery time (Marshall, De Busser, and Hesselman). An organisation, therefore, wants to measure how long it takes to recover from an attack. Linkov and colleagues (2013-b) suggested assessing the distance to functional recovery. However, this research will argue for the aspect of a system to record the recovery time. Although functional recovery is reasonably easy to accomplish, as we discussed earlier, a measurement of how long the services were down is important (Marshall, De Busser, and Hesselman). Thus, the organisation will have a device to measure this in the physical domain. Later, the corresponding chapter will explain how the organisation's loss will be calculated using this measurement in the cognitive domain.

De Busser asked: *'Do you have to be 100% operational again, or is 70% also good enough?'* This reasoning is in line with the statement of Niemantsverdriet: *'Maybe you could look at whether you can run the website or application on a reduced functionality.'* This questioning to deliver the organisation's functionality in a reduced version could enable the organisation to be, although limited, functional again. Although this research will reason about the organisation's functionality in the cognitive domain, this domain will need to cover the implementations on how to recover from a DDoS attack with reduced functionality. Then, the fourth aspect in this domain is Implementations to recover with reduced functionality. To what extent this functionality is reduced or to what extent it can be reduced depends on decisions made in the cognitive domain. Section 3.3 will cover this more thoroughly in its recovery phase.

3.1.4 Adaptation phase in the physical domain

Linkov and colleagues (2013-b: 474) provide two aspects for the adaptation phase in the physical domain: *'review asset and service configuration in response to a recent event'* and *'phase-out obsolete assets and introduce new assets'*. The researchers determined this phase as where the victims use the knowledge about the event to alter the configuration of the system. In this phase, the respondents suggested the aspects a Review of assets and service configuration in response to the recent event and a Phase-out of obsolete assets and an introduction of new assets.

The first aspect is a review asset and service configuration in response to a recent event. For example, it could be a specific device that did not respond appropriately to the attack, and the organisation will replace it (Van der Kraan). The respondents also suggested models that

approach the adaptation structurally, but those will be discussed more thoroughly in the cognitive domain. In this domain, a respondent put forward the organisation's capabilities to mitigate a DDoS attack (Marshall). He noted: *'Unless you can buy a couple of hundred Gigabits per second in bandwidth and spend hundreds or tens of millions of euros in hardware. But, who can do that? Even the richest companies who have a billion in profits every quarter do not see that as a good investment. They rather spend 10 million on people and provide good products.'* Again, an organisation should consider its possibilities to mitigate DDoS attacks on their own.

After the organisation assessed the current system's performance during the attack, the organisation will have to adapt to cover a comparable attack in the future. Almost all respondents specifically argued in line with this reasoning (Niemantsverdriet, Van der Kraan, Schaapman, De Busser, Marshall, Pras, Hesselman). Therefore, this research includes a phase-out of obsolete assets and an introduction of new assets as the second aspect in this phase.

3.1.5 Conclusions on the physical domain

The previous chapters discussed the relevant aspects of the physical domain and found aspects in all phases to a total of twelve aspects. Table 6 illustrates the aspects of the physical domain over the different phases.

In the planning and preparation phase, the respondents argued for aspects comparable to those of Linkov and colleagues (2013-b). The aspect of *'assessment of network structure and interconnection to system components and to the environment'* is renamed to mapping the network structure. This aspect does not necessarily concern an assessment or review, and now the aspect is measurable. The aspects *'implement controls/sensors for critical assets'* and *'implement controls/sensors for critical services'* of Linkov and colleagues (2013-b: 474) are renamed to mitigation systems and detection systems.

Moreover, this research does not concern whether the mitigation and detection systems are protecting assets or services. Those systems will protect against different types of DDoS attacks and prevent the loss of availability. Whether that availability is that of an asset or service does not matter in this research. On the other hand, this research does differentiate between detection and mitigation measures and divides them into two aspects.

Then, this research adjusts the imperative form of the aspects of Linkov and colleagues (2013-b) to make them measurable. Advising an organisation to implement controls or sensors is not a quantifiable aspect. Moreover, this research considers separation as an independent

aspect as it does not mitigate or detect a DDoS attack. Instead, when done correctly, it will decrease the effect of a DDoS attack.

Then, the respondents came to working mitigation and detection systems in the absorption phase. Unlike Linkov and colleagues (2013-b) 'Signal the compromise of assets or services', the aspect of working mitigation and detection systems is that the aspect of this research includes a check of whether the systems are functioning correctly. In addition, the systems will issue a signal when working correctly.

Moreover, this research did not include the redundancy and dedication of cyber resources of Linkov and colleagues (2013-b). Those are covered in the detection and mitigation systems of the planning and preparation phase. In the absorption phase, those aspects are checked with the aspect of working mitigation and detection systems. A new aspect resulting from this research is a tracker of the response time.

On the other hand, this research came to comparable aspects as Linkov and colleagues (2013-b) in the recovery phase. The main differences are the restating the aspects from imperative statements to actual aspects and the required functionality. The latter requires the organisation at which level the systems need to be functional. Linkov et al. (2013-b) did not cover this in their matrix.

Finally, this research stayed with Linkov and colleagues (2013-b) aspects in the adaptation phase. The respondents and literature did not involve other aspects but did agree with the aspects of the researchers.

Table 6: Aspects of the physical domain

	Plan/prepare	*Absorb*	*Recover*	*Adapt*
Physical domain	Mapping on the network structure	Working mitigation and detection systems	Assessment of service/asset damage	Review of assets and service configuration
	Mitigation systems	Sufficient separation	Reparation or replacement of damaged assets	Phase-out of obsolete and introduction of new assets
	Detection systems	Tracker of the response time	Reparation or replacement of malfunctioning systems	
	Separation of the network		System to measure the recovery time	
			Required functionality	

3.2 The Information domain

The information domain in the matrix of Linkov and colleagues (2013-b: 473) is concerned with the *'Information and information development about the physical domain'*. In the next subchapters, this research describes the phases of this domain and the interviewees' responses.

3.2.1 Planning/preparation phase in the information domain

In line with the reasoning of Linkov and colleagues (2013-b: 474), an organisation should consider five aspects during this phase: *'categorize assets and services based on sensitivity or resilience requirements'*, *'documentation of certifications, qualifications and pedigree of critical hardware and/or software providers'*, *'prepare plans for storage and containment of classified or sensitive information'*, and *'identify external system dependencies (i.e. Internet providers, electricity, water)'*. The respondents also reasoned about this phase. One respondent even confirmed the relevance of all aspects presented by Linkov and colleagues (2013-b) (Marshall). Based on their responses, this research comes to one or more Locations to store data gathered during a DDoS attack, Separation of data storage, Sharing possibilities, Retrieving possibilities, Standardised storing method, a Profile of normal traffic, Access rights, and Encryption.

The first aspect of this domain is a location to store gathered data (Niemantsverdriet). Like the physical domain, the organisation would like to have copies of the data stored at separate locations (De Busser and Marshall). An organisation might improve its resilience by replicating data over several databases. In that way, if one database gets compromised or not available, the organisation can still retrieve the data. Therefore, this research considers the aspects locations to store data and the separation of data locations.

A resilient organisation then implements possibilities to share data and information (Niemantsverdriet, Van der Kraan, Pras De Busser, Marshall; Fox-IT, 2020; Boin et al., 2017). For example, as we will find out in the social domain, more resilience follows if an organisation commits to cooperation. An organisation in cooperation will share information and can prepare for attacks that happened somewhere else.

Another example might be that the organisation is obligated by law to share information with others. Those are examples of stakeholders that might need to be informed. This research discusses all of those in the social domain. In this domain, it is relevant to have the possibilities to share the information with others. Therefore, this research includes the amount of data sharing connections with stakeholders as a second aspect.

The research of Kulikova, Heil, Van den Berg, and Pieters (2012) offered a decision-support framework for disclosing security incident information. This framework would guide organisations step-by-step to address challenges and develop an appropriate incident disclosure strategy. A sufficient strategy would lead to timely and consistent communications, and avoid confusions, rumours, and a sell of company's shares (Kulikova, Heil, Van den Berg, & Pieters, 2012).

Similarly, an organisation wants to retrieve information about DDoS attacks from others (Niemantsverdriet). The sense-making task of Boin et al. (2017) includes the task of sharing information. In that way, the organisation will get insights on attacks based on other organisation's data (Hesselman) which enables the organisation to detect and mitigate attacks faster (Schaapman). This research identifies, therefore, information retrieval possibilities as the third aspect of resilience.

The organisation will need a standard to share and retrieve information efficiently (Niemantsverdriet). This research identifies a standard for organising and sharing information as a fourth aspect. Fortunately, the DDoSDB has made a tremendous effort in facilitating an interface for searching unique characteristics of attacks (Schaapman, Pras, and Hesselman). These characteristics are called DDoS fingerprints and are not a new topic in research (Lee & Shieh, 2005; Fachkha, Bou-Harb, & Debbabi, 2014; Osanaiye, 2015; Ahmzed, Ullah, & Kim, 2018). That collaboration provides data sharing via an open-source code that analyses attack, generates fingerprints, and anonymizes the victim's identity (DDoSDB, n.d.). If an organisation is committed to collaboration, this will influence the standard the organisation will follow. This research will elaborate more on this collaboration and others in the social domain.

So far, this phase consists of locations to store data gathered during a DDoS attack, separation of data storage, sharing possibilities, retrieving possibilities, and a standardised storing method. The fifth, sixth, and seventh aspect are a profile of normal traffic, access rights, and encryption. This chapter will discuss those next.

This research considers a 'normal' profile as an aspect of the resilience in the information domain. As discussed in the physical domain in the preparation phase, anomaly detection devices will compare the potential malicious traffic to the 'normal' profile associated with the organisation. If an organisation chooses to outsource the mitigation of DDoS attacks, this second organisation will likely need this information to involve their anomaly detection devices (Schaapman). A more resilient organisation ought to keep track of this profile.

The sharing of information requires the organisation to involve access rights (De Busser) or identity and access management (Marshall). In most cases, an organisation would like to share some information with one of its department but not with another organisation. Therefore, an organisation would provide different access rights. The social domain sets out to which actor an organisation will provide certain information.

If an organisation wants to unable the access to data for certain actors, it will also encrypt its data (Marshall). Thus, this research includes data encryption to the aspects of the information domain.

For the above two aspects, an organisation uses those to keep information confidential. The CRAC: Confidentiality Risk Analysis and IT-Architecture Comparison of Business Networks model of Morali, Zambon, Etalle, and Wieringa (2009) provides organisation insights on assessing and comparing confidentiality risks of business networks. According to those researchers assessing those risks is particularly challenging in cross-organisation cooperation, something this research will also address in the social domain.

So, this research puts seven aspects forward. This research does not include *'categorize assets and services based on sensitivity or resilience requirements'* like Linkov and colleagues (2013-b: 474). Those researchers made a mistake by having this aspect in the information domain, although a categorisation would better fit the cognitive domain. This research will explain this more thoroughly in the corresponding chapter.

3.2.2 Absorption phase in the information domain

In the absorption phase of the information domain, aspects for measuring the resilience are: *'observe sensors for critical services and assets'* and *'effectively and efficiently transmit relevant data to responsible stakeholders/decisionmakers'* according to Linkov and colleagues (2013-b: 474). The respondents suggested a Real-time monitor tracking the network volume, a Signal, Capacity to store log files, Informing authorities and relevant vendors, and a Threshold for valid information.

The first aspect is comparable to the aspect '*observe sensors for critical services and assets'* of Linkov and colleagues (2013-b). A respondent argued for tracking the volume of the network traffic (Niemantsverdriet). The organisation is monitoring the traffic via the detection devices. This requires an organisation to have some real-time monitoring system in place (Schaapman).

Secondly, if an organisation uses the NaWas, then the organisation will also receive information from the NaWas in their monitoring system (Schaapman). Thus, whether the

organisation mitigates a DDoS attack on their own or outsource the mitigation to a CDN service provider, the organisation would need a monitoring system in place which can also include information provided by other organisations.

Therefore, the organisation would like to get a signal whenever a potential DDoS is initiated. This signal would alert the organisation and enables it to respond quickly. This signal can be generated by the monitoring system or via another system. This does not matter to this research, but it will consider whether the information domain gives a signal based on the devices' data in the physical domain.

The fourth aspect is storing log files on the storage capacity that the organisation would have made available during the preparation phase (Niemandsverdriet). This possibility can also be a feature of the monitoring system.

Not surprisingly, the organisation informs involved authorities and vendors (Van der Kraan). Those authorities and vendors will need DDoS signatures and a profile of the normal traffic (Schaapman). Therefore, this research considers informing authorities and vendors as an aspect of this phase.

Finally, the organisation will have to determine the information's validity as it comes in. What starts as a hypothesis has to become a fact. The organisation must have procedures in place to determine the validity of incoming information (Niemantsverdriet). The organisation would implement thresholds for valid information. This could be a number of different parties or employees retrieving identical information, or the information could come from a reliable source.

3.2.3 Recovery phase in the information domain

'Log events and sensors during event' and *'review and compare systems before and after the event'* are the two indicators for measuring resilience in the recovery phase in the information domain according to Linkov and colleagues (2013-b: 474).

A few respondents provided aspects that belong to this phase in the information domain (Niemantsverdriet, De Busser, Marshall, and Hesselman). This could be the result of the ambiguity in Linkov and colleagues (2013-b). This research will elaborate more on this in chapter 4. Also, the aspects *'review and compare systems before and after the event'* of this phase and *'document incident's impact and cause'* of the Adaptation phase tend to overlap (Linkov et al., 2013-b: 474) as both actions are about analysing what went wrong and how it impacted the organisation's system.

The respondents provided the indications Securing log files and the Use of standards in languages to describe cyber threat information (CTI) and protocols for exchanging CTI over the Internet.

The first indication is whether the log files are secured. The organisation will need to make sure the system does not overwrite the information of a previous attack with data from the next day or the next attack (Niemantsverdriet, Van der Kraan, Marshall). The organisation will need to retrieve information from an attack, and make an effort to assure the data is not lost somewhere.

Another aspect is the use of standards in languages to describe cyber threat information (CTI) and protocols for exchanging CTI over the Internet. For example, a respondent recommended looking at STIX and TAXII (Hesselman) (OASIS, 2020-a; 2020-b). Another respondent suggested the MITRE ATT&CK framework (Niemantsverdriet). This framework of tactics and techniques used by red teamers, threat hunters, and defenders to better classify attacks (MITRE, n.d.). In a blogpost, Fox-IT also frames the adversary's work in the MITRE ATT&CK framework (Fox-IT, n.d.). By implementing such standards, organisations can efficiently communicate with each other, understand it faster, and interpret the information more quickly.

3.2.4 Adaptation phase in the information domain

In the Adaptation phase in the information domain, research suggests to *'document incident's impact and cause'*, *'document time between problem and discovery/discovery and recovery'*, *'anticipate future system states post-recovery'*, *'document point of entry (attack)'* (Linkov et al., 2013-b: 474).

The respondents of this research came to five aspects. Those are a Debriefing, Information to adopt, an Information share with partners, an Addition of the information from partners, and an Addition of information of intelligence.

The first aspect in this phase is to document findings based on the previous phases' log files and come up with some debriefing. This activity includes to map the attack entirely, its target, and determine what happened when (Niemantsverdriet, Van der Kraan, Schaapman, De Busser, and Marshall; Fox-IT, 2020). After a large incident, a telecommunications operator typically executes an incident analysis to prevent future incidents (Wienen, Bukhsh, Vrizekolk, & Wieringa, 2019). The research of Wienen et al. (2019) investigated a DDoS incident with

the AcciMap method and found that it yielded many recommendations. Therefore, this research includes a debriefing in the matrix.

Another example is that the NaWas records all the attacks they get in terms of the type of attack, the target, and the mitigating rules they used (Schaapman). This research includes such recording in an incident report and also the impact of the attack. This can be expressed in how many connections were lost, how many customers could not connect, transactions that failed, lost expected revenue, or profit (Marshall). However, some of this information will be hard to obtain. One respondent noted that it is challenging to *'document point of entry'* even after forensic investigation, even though Linkov and colleagues (2013-b: 474) put this aspect into their framework (De Busser).

Secondly, it is vital to subsequently adapt based on this incident report (Niemantsverdriet and Marshall). If the organisation does not adapt to the discoveries of the incident, then the organisation will stay vulnerable to a comparable attack. To prevent this, this research includes information to adjust according to the findings of the debriefing.

Then, an organisation would potentially like to share the information in that incident report with other actors such as CDN services providers (Van der Kraan; Fox-IT, 2020), investigating services (Niemantsverdriet), or parties belonging to the anti-DDoS collaboration in which the organisation is potentially participating in (Pras). In partnerships, it is not only about consuming but also contributing information. It is appreciated if an organisation can contribute to the knowledge within the collaboration (Pras). As soon as a new type or a combination of types comes in, those other actors can mitigate the attack sooner.

Likewise, an organisation would also include information of others into its knowledge (Niemantsverdriet). CDN services providers regularly release reports, or the organisation could search for information on the Internet (Van der Kraan). A respondent noted that most CDN services providers are not likely to share all details on mitigating DDoS attacks (Schaapman). After all, it is their business model to deliver a paid DDoS mitigation service. This research will not advocate for or against paid services, but an organisation will have to determine the extent to which it wants to obtain information on DDoS attacks and resulting mitigation methods. Other information to include are threat reports of Europol, Interpol, Kaspersky, or Symantec (De Busser). The fourth aspect in the phase is, therefore, the amount of information from external organisations.

According to one respondent, an organisation should look at what it gathers from data and correlate that with its intelligence (Marshall). He stated: *'Should you have known about it*

before it happened? What was out there before the day on which the organisation got attacked? Has the organisation ignored things?' This research considers this, the addition of information from own intelligence, as the fifth aspect of this phase. This facet also includes out-of-the-box thinking. According to another respondent, the organisation should try to get into the head of the attacker and come up with tomorrow's potential threats (De Busser). In doing so, the organisation could include information from threat reports of organisations like Europol, Interpol, Symantec, and Kaspersky (De Busser).

Moreover, one crucial reason for not using data is having too much (Marshall). In some cases, data are abundant. It is easy to log everything, but it is challenging to put it into something usable. The organisation would need a team that works on this processing. The research will cover the specific interpretation of this team in the social domain.

3.2.5 Conclusions on the information domain

In the previous chapters, the aspects of the information domain have been discussed. With a total of nineteen aspects, those chapters found aspects in all of the phases. Table 7 illustrates the aspects of the information domain over the different phases.

First of all, the research did not include the categorisation aspect of Linkov and colleagues (2013-b) in the planning and preparation phase of the information domain. As explained, this research will cover that in the cognitive domain as it is a better fit there.

Moreover, this research included sharing and retrieving information. Sharing data and information with others would improve resilience. The organisation does not have to sort everything out on its own. Frankly, Linkov et al. (2013-b) did not include those aspects in their research. This study will explain more about collaborations and partnerships in the social domain.

Compared the Linkov and colleagues' (2013-b) matrix, this research underlined the importance of real-time monitoring the system and retrieving a signal when things go wrong during the absorption phase besides the only observation of sensors. It also includes the capacity to store log files and the informing of authorities and relevant parties.

The most prominent discovery is a threshold for valid information. With this aspect in place, the organisation would gather information and share it with others and determine how much the information is worth.

In the recovery phase, this research found that besides the logging of events proposed by Linkov et al. (2013-b), the organisation should also determine which standards and protocols it will use to describe CTI and exchange information.

Finally, this research put the aspects of the documentation of an incident's impact and cause and time between discovery and recovery in the aspect of a debriefing of the adaptation phase. Besides the improvement of fixing the imperatives in Linkov and colleagues (2013-b) aspects, this research also emphasised learning from information of others and sharing information.

Table 7: Aspects of the information domain

	Plan/prepare	*Absorb*	*Recover*	*Adapt*
Information domain	Locations to store DDoS data	Signal	Securing log files	Debriefing
	Separation of data storage	Capacity to store and log files	Standards in CTI language and exchange	Information to adopt
	Sharing possibilities	Informing authorities and relevant vendors		Information share with partners
	Retrieving possibilities	Real-time monitor		Addition of intelligence
	Standardised storing and sharing	Threshold for valid information		
	Profile of normal traffic			
	Access rights			
	Encryption			

3.3 The Cognitive domain

Linkov and colleagues (2013-b: 473) describe the cognitive domain as *'use of the information and physical domains to make decisions'*. This research describes the different phases in this domain in the following subchapters.

3.3.1 Planning/preparation phase in the cognitive domain

Linkov and colleagues (2013-b: 474) suggest three aspects in the preparation phase of the cognitive domain. Those are *'anticipate and plan for systems states and events'*, *'understand performance trade-offs of organisational goals'*, and *'scenario-based cyber wargaming'*.

Based on the respondents' answers during the interviews, this research comes to a Mapping of the service, Key Performance Indicators of the service, a Crisis plan, and Scenario-based testing and rehearsal.

The way the organisation will be defending its system depends on its service (Schaapman). Therefore, the first aspect is a mapping of the organisation's service. This aspect comprises the popularity of the service (Schaapman), who the customers are (Pras), whether

they are as distributed around the world as attackers (Pras), and the impact of the service being down for a particular time (Schaapman, Pras). Then, the organisation should question *'How critical are all of your systems?' 'What are the underlying systems?'* And *'on what do those systems run?'* (Niemantsverdriet). In addition, This aspect also includes *'categorize assets and services based on sensitivity or resilience requirements'* that Linkov and colleagues (2013-b) put in the information domain and determines the expectations of a company's resilience to DDoS attacks.

For example, what is expected from a small organisation versus a bigger one? Then, the organisations will fulfil resilience differently (De Busser). This all has to do with the organisation's identity, size, scope, and budget.

Moreover, one respondent argued that many reasons why actors start to attack organisations are because of the organisation's business and how much attention they attract to themselves (Marshall). If an organisation is attacked with a DDoS off the shelf, a DDoS-as-a-service, the organisation is probably doing something that is not particularly nice. As a result, people do not like the organisation and want to harm it.

Comparably, Kumar and Carley (2016) studied the sentiment in Twitter posts to observe country-to-country perceptions and found that the probability of attacks increased by up to 27% while experiencing negative sentiments from other nations.

Another example would be that the organisation has made a severe mistake and ends up on all of the newspapers' front pages (Schaapman). An organisation could benefit from this aspect by adjusting its security when planning to make such investments or getting involved with activities that others could perceive as immoral.

This aspect also includes the other parties contributing to the service (Niemantsverdriet). Is it possible to get those in line if something is going on? What arrangements are in place, and what is agreed upon concerning the server levels and support? Also, the organisation should contemplate itself. For example, do customers expect a small organisation to be very resilient against DDoS attack? So, the size, identity, and budget all play a part in this (Niemantsverdriet, Pras, Schaapman, De Busser). Is a DDoS attack something that would directly harm the organisation or at most affects it a bit but does not have a real business impact?

Based on this information, the organisation should come to Key Performance Indicators (KPIs) of their service (Pras). Based on those indicators, an organisation would determine how much of their service is down. This information enables the organisation to plan for

performance trade-offs during a DDoS attack. This aspect links to the physical domain and indicates what has to be done in the physical domain to make the service running again. Therefore, the second aspect is the KPIs of the organisation's service.

Also, the organisation should question when its service needs to be online (Pras). For example, if an online store primarily sells products during the day in a specific country, it will not have many losses when a DDoS attack puts its systems down during the night. On the other hand, if the organisation is a bank and payment transactions must continue day and night (Pras). Then, the organisation must have an arrangement if something happens at night as well, and there will always be people responsible and able to respond (Pras).

Furthermore, the interviews suggested that the organisation's resilience will benefit from a crisis or response plan covering the steps to be made while under an attack (Niemantsverdriet, Pras, Hesselman). The cybersecurity company Fox-IT also addressed this in its guide *'Prepare and Respond: The Guide to Cyber Incident Response Planning'* and advises to create a cyber incident response plan in six steps (Fox-IT, 2020). Therefore, the organisation would have procedures and decision support tools in place to assist during the attack (Hesselman). A respondent also advocated for a contingency plan on a national level (Pras). Hesselman specifically suggested the DDoS cookbook and also ISO27001[2]. The DDoS cookbook is a project of SIDN, SURF, and the University of Twente together with parties like Telecom Italia as part of CONCORDIA[3]. Based on the lessons learned from setting up the anti-DDoS-coalition in the Netherlands, this project provides technical, legal, and organisational insights on setting up coalitions (Hesselman, Poortinga-van Wijnen, Schaapman, Ruiter, 2020).

According to several respeonds, testing is vital for determining the organisation's resilience (Niemantsverdriet, De Busser, Van der Kraan, Marshall). Niemantsverdriet even argued for testing whenever possible (Niemantsverdriet). Therefore, this research includes scenario-based testing as an aspect to determine the resilience of an organisation. The organisation would reason about how attackers could proceed with their attacks. This aspect is dependent on the organisation's service and the mapping provided in the physical domain (Van der Kraan, Pras, Schaapman).

A respondent divided the potential group of attackers into script kiddies, (pseudo-)professionals, and nation-states (Pras). All have different resources and skills available and can perform various kinds of DDoS attacks or perform them with other volumes (Pras, Van der

[2] ISO27001: https://www.iso.org/isoiec-27001-information-security.html
[3] CONCORDIA: https://www.concordia-h2020.eu/

Kraan, Schaapman). For example, the schooling sector has to deal with DDoS attacks from script kiddies, who try to take down digital exams. Their attacks are relatively easy to mitigate (Schaapman). With professional attacks, it is likely to see phasing and extortion. In that case, the attackers could perform a DDoS at night to show their power and issue a warning. The attackers start pressuring the victim and perhaps send a ransom note (Schaapman). In Augst 2020, Akamai tracked ransom demand DDoS attacks from criminals claiming to be part of the Armada Collective and Fancy Bear (Akamai, 2020). The combination of DDoS and ransom thus occurs. On the other hand, nation-states are often quite blunt, *'rücksichtslos'*, and relatively coarse. They will try to undermine vital routes and influence as many parties as possible (Schaapman).

To illustrate the difference, a nation-state would not bother to target a specific small webstore. If a nation-state wants to attack, it would instead focus on the Netherlands as a whole. It is then no longer a matter for individual webstores in the Netherlands, but rather the central government (Pras). A single organisation would, therefore, consider the relevance of protecting against nation-states. DDoS attacks from nation-states are a potential danger, as shown by the study of Thornton-Trump (2019) on the politics of cyber. In that study, the researcher laid out the development of nation-state capabilities and the cyber policing role of the U.S. and its extraterritorial jurisdiction (ETJ) authority outside its borders.

The study of Almeida, Doneda, & De Souza Abreu (2017) provided definitions and categories of cyberwarfare. Although their scope is broader than DDoS attacks, their findings on the legal treatment of cyberwarfare and the relationship between cyberwar and Internet Governance are engaging.

One respondent specifically argued against the use of the word script kiddies (Marshall). He does not like the term because there is nothing stupid about kicking off a DDoS attack. *´It takes intelligence; it takes organisation and effort.'* The term trivialises the phenomenon, and that can only work out for the worse.

Based on the information the attackers could find on the Internet about the organisation and its system, the attackers determine their approach of performing a DDoS. Based on the kind of DDoS attacks attackers are using, the organisation sets out different attack scenarios. For example, the organisation could question: *'What kinds of attacks are there? Which attacks are commonly used? Are we protected from those, yes or no?' Well, let's see through a test.'* (Van der Kraan). Then, the organisation test its systems by re-enactments of these scenarios. This testing is comparable to fire drills twice a year (Niemantsverdriet).

Marshall provided other related aspects such as protection scenarios, wargaming, red teaming, blue teaming, and purple teaming. This research encapsulates all of those in the notion of scenario-based testing. A variant of testing is chaos engineering. It includes taking servers down at random moments and making entire parts of the network unavailable (Niemantsverdriet). This testing method is based on ensuring that the systems and people are continuously trained to deal with disruptions. Fox-IT also suggests testing policies and procedures (Fox-IT).

To test its systems, the organisation can do this by simulating attacks. The organisation could outsource this to other companies such as Computest (Niemantsverdriet), but should do business with booter or stressor sites (Van der Kraan, Pras). Those sites sell its services online enabling offenders to launch attacks, so-called DDoS-as-a-service. Musotto and Wall (2020) and Hyslip (2020) analysed those DDoS booter sites thoroughly. The researchers explored the service operations and payment systems and found that the business model is comparable to legitimate e-commerce websites in the way of product, price, and costumers. Those sites remove the technical barrier to carry out DDoS attacks (Santanna et al., 2017). Anyone can start a DDoS attack for affordable prices, starting from less than five dollars. The research of Noroozian et al. (2016) examined the most significant victims of these booter sites.

Those booter sites can be assessed on the Dark Web. People can visit this obscure part of the Internet with anonymising tools such as The Onion Router (Tor). The study of Takaaki and Atsuo (2019) created a picture of the Dark Web including DDoS services but also the trade in drugs and weapons, child pornography, and sensitive information such as credit card information.

If affiliated with the anti-DDoS working group[4], an organisation can also test with other participants (Pras, Hesselman). The involved organisations could agree to attack each other's systems. An example would be that multiple organisations perform a DDoS attack on one other participant in the working group. Most of them are currently announced beforehand as the attack could otherwise result in too many losses (Hesselman). Either way, the DDoS-performing organisation would need a considerable capacity to do so (Pras).

Even if emulations of DDoS attacks are not possible for the organisation, exercises on paper would be beneficial too (Niemantsverdriet). Key is to rehearse or practice the plans and procedures and make the organisation run smoothly when the system gets attacked for real.

[4] Nationale Anti-DDoS-coalitie: https://www.nomoreddos.org/

The advantage is in the outcome of those re-enactments as the organisation can find out practical things are missing or no longer being up-to-date in their plans and systems.

Van der Kraan laid out the relevance of the aspect as he pointed out that the organisation's resilience can only be determined by testing. Marshall put it like this: *'If you can test, you can verify'*. The organisation would also indicate the impact of different attackers in terms of the KPIs presented as the second aspect in this chapter or organisational goals (Niemantsverdriet). For example, the NBIP always performs a DDoS test with every new participant as an intake. They would go through the whole procedure to make sure the participants know what they can expect from NBIP and vice versa.

Besides, if the organisation is about to implement changes in their system, the question would be whether the system can parry the attacks that it could before the update (Van der Kraan).

3.3.2 Absorption phase in the cognitive domain

The absorption phase has four aspects to consider when following the resilience matrix (Linkov et al., 2013-b). Those are *'use a decision-making protocol or aid to determine when event can be considered "contained"'*, *'the ability to evaluate performance impact to determine if mission can continue'*, *'focus effort on identified critical assets and services'*, and *'utilize applicable plans for system state when available'* (Linkov et al., 2013-b: 474).

The respondents came to Determination of the incident as an attack, Decision-making protocols, the Following the plan, a Determination of whether the attack is over, and a Consideration that the DDoS acts as a smokescreen for this phase in the cognitive domain.

The first aspect of this phase is questioning whether the attack actually is an attack (Niemantsverdriet, Van der Kraan). Maybe the traffic and volume will increase a lot, but the organisation could be offering a service that people use during that time. Niemantsverdriet provided an example: *'If your organisation offers a service that people use during their lunch break and you always see a huge peak between 11.30 and 13.00, you do not want to block that traffic'*. So, the organisation would compare the potential attack's traffic with that of a normal situation.

Another aspect that should be considered is making decisions efficiently. According to Boin et al. (2017), decision-making is one of the crisis management task domains. In most cases, it is most beneficial to automate as much as you can (Van der Kraan, Marshall). Thus, this means making data-driven decisions. The best news is getting a call informing the attack

is already mitigated. The organisation could also use decision support or intelligent tools that calculate the results of different decisions (Hesselman).

On the other hand, manual decisions are inevitable in some cases. Specific cases will need customised approaches because the organisation could take too drastic measures that impact customers (Van der Kraan). This aspect could also be considered as crisis management (De Busser). This research finds a decision-making protocol as the second aspect to cover the whole issue, including automated and manual decisions.

When there is a new situation going on, you often find yourself in situations where you know relatively little and make decisions quickly (Niemantsverdriet). It is then very tempting to say we do not see the problem very well, so if we investigate a few more hours further, we will know more and make a better decision. However, this does not guarantee a better decision while taking more time to come to a decision (Niemantsverdriet). The organisation will need to have procedures or a decision-making protocol to determine when enough valid information is enough to make decisions without a full story (Niemantsverdriet).

This research already underlined the importance of deciding which information is valid and determined that in the information domain. The aspect a threshold for valid information in the absorption phase encompasses this notion.

When considering the amount of valid information, one respondent argued it could be a threshold (Niemantsverdriet). Another method could be to make the response team come together at a particular frequency cadence. When the team comes together, they make the decisions based on the information available to them (Niemantsverdriet). Also, the team's composition in charge can change if the situation becomes more severe than before, and the organisation would need to consider that the team is fallible and take measures accordingly. This research examines these considerations more thoroughly in the social domain.

Thirdly, an aspect in this phase is to follow a plan, procedures, or a runbook that were laid down in advance (Niemantsverdriet, Marshall, Pras, Hesselman). Those plans will need to cover which actions have to be taken in case of an attack. All of the other domains come together in this domain as people from the social domain will be executing the plan, their acts are based on the insights of the information domain, and they adjust the system in the physical domain. Those plans can be based on standards to comply with potential regulations.

Another aspect is to determine when the attack is over. In essence, when the organisation’s service comes back online, then the attack is either repulsed or aborted (Van der Kraan, De Busser). The latter is essential as it is possible the attacker stops to pause for a

moment and continues the attack later on. Van der Kraan put it like: *'Well, I'll take a sip of my coffee and then I will attack again.'* The attacker could also use this pause to send a ransom email. In such a case, the attacker intended to deter and demonstrate his abilities (Van der Kraan, Pras). There have also been some occasions where the attackers try to perform different types of DDoS attacks (Schaapman). It is up to the organisation to see the type of attack and quickly deal with it while the attack type changes. The issue then becomes a race in the attackers turning their buttons and the organisation its controls in response.

This research also considered the possibility of covering the mitigation of DDoS attacks to a certain degree and leaving bigger or more complicated ones to other organisations. This research included this in the physical domain and will cover the agreements with other organisations in the social domain. In this domain, the organisation considers the amount it would like to mitigate DDoS (Schaapman). Since the respondent's scepticism towards organisations being able to cover even the most significant DDoS attacks, organisations will likely have to consider to which degree it wants to mitigate attacks themselves. This consideration will be a trade-off between the investments to mitigate a DDoS attack and the costs of the third parties' services.

Finally, the organisation should keep in mind that attackers could use a DDoS attack as a smokescreen (Niemantsverdriet, Van der Kraan). The DDoS attack would then be an opportunity to create a distraction to initiate another attack while the victim's defensive team is mitigating the DDoS (Newman, 2019; EESC, 2018: 23). This research also underlined and explained this phenomenon in the theoretical framework.

3.3.3 Recovery phase in the cognitive domain

In the recovery phase in the cognitive domain, Linkov and colleagues (2013-b: 474) argued for the following two aspects: *'review critical points of physical and information failure to make informed decisions'* and *'establish decision making protocols or aids to select recovery options'*.

The respondents came to a Review of the plans and procedures and Reputation for the recovery phase in the cognitive domain based on the responses to the interviews.

The first aspect is a review of the plans and procedures (Niemantsverdriet, Van der Kraan, Marshall, Hesselman). The organisation will document its findings and maps out the DDoS attack completely covering what happened when. The organisation should do this after attacks and also after DDoS tests (Van der Kraan). The organisation needs to question what

steps it took and what it did differently in reality compared to the plan? And did this work turn out to be for the better or worse? (Marshall). Advantages would be the organisation has the information available during the next attack and the possibility to learn from the attack. The latter is also vital for the Adaptation phase covered in the next chapter.

Secondly, according to Marshall, the aspect of reputation is of importance. Unfortunately, the reputation of an organisation is challenging to measure. He stated: *'Reputation generally becomes measurable when you do something horrible, and then everyone hates you forever'*. An organisation wants to keep its reputation or customer satisfaction intact, even after a disastrous DDoS attack. Keeping its reputation in mind, an organisation would disclose responsibly, be honest, take its punishment well, and put the government and customers first. This final remark extends into the information domain.

3.3.4 Adaptation phase in the cognitive domain

The model of Linkov and colleagues (2013-b) suggests *'review management response and decision making processes'* and *'determine motive of event (attack)'* as the aspects of this phase in the cognitive domain.

On the other hand, the respondents of this research suggested a Depreciation of response plans, a Potential adjustment in plans and procedures, a Tracking of incidents and impacts, and a Rough indication on the type of attacker.

The first aspect to take into consideration is some depreciation of response plans (Niemantsverdriet). As time passes by, attackers change their behaviour, and their attacks become more sophisticated. Plans of some years ago will no longer be up-to-date and need revision after some time. This research includes the depreciation of response plans and encourages organisations to update their plans to compensate for this. Whether the organisation has fallen victim to a cyberattack or not, it should review its management processes or responses (De Busser).

Secondly, after an incident has taken place, it is essential to see what went well and what went wrong. This research already covered the incident's log files in the information domain, but in this domain, the organisation uses this information to work to lessons learned (De Busser). This phase in this domain underlines the need to improve plans and procedures. The organisation will implement adjustments during this phase if necessary (Niemantsverdriet, Van der Kraan).

Another aspect is keeping track of the number of incidents and corresponding impact taking place (Niemantsverdriet). Are those on the rise or decreasing? Here also the threat intelligence comes into play (Marshall). The same can be said about the impact of those incidents. However, there is a catch in this. It almost becomes a philosophical discussion whether it is better to have a lot of smaller attacks with little impact, causing the organisation to be alert for bigger attacks or not have those smaller incidents at all (Niemantsverdriet).

To illustrate, if the organisation keeps track of the number of incidents with an impact, then the first scenario could be worse for the organisation, although the benefit would be preparedness of the organisation for the more significant attack. It is challenging to determine whether the effects of a lot of smaller attacks outweigh the impact of one or a few more significant attacks. Therefore, this research would not recommend attaching reviews based on the number of incidents and their impact but to determine whether improvements are necessary to prevent impact in the future.

Fourthly, it is hard to determine the motive of the attack (Van der Kraan, De Busser, Marshall, Pras). The attacker could be motivated by making money through a ransom (KPN, n.d.), but there are many possibilities, as discussed in the introduction. Therefore, it is doubtful how much finding out the motive of the attack will influence the system's resilience. Moreover, the policy brief *'Three tales of attribution in cyberspace'* by Broeders, De Busser, and Pawlak (2020) pointed out that attribution, or the search for evidence to discovering who is responsible and which individual(s) should be prosecuted, requires technical and high-end intelligence capabilities. As such, it is already challenging to find a perpetrator, let alone the perpetrator's motive.

On the other hand, there is something to say about the kind of actor behind the attack combined with the volume of the attack (Van der Kraan, Pras). This research already covered this in the preparation phase of this domain. However, in this phase, the organisation would use the probable kind of attacker into consideration here and update their systems based on potential attacks from that same kind of attacker. For example, if an organisation just mitigated an attack which is likely to be caused by a script kiddie. Then, the organisation would like to adjust their systems to be resilience to similar attacks caused by the same kind of attacker.

3.3.5 Conclusions on the cognitive domain

Based on the interviews and literature, the previous chapters suggested fifteen aspects of the information domain. Again, the results proposed aspects in all phases and table 8 includes the aspects over the different phases.

In the planning and preparation phase of this domain, this research found that most of the aspects of Linkov and colleagues (2013-b) are applicable to resilience to DDoS attacks. The three aspects of those researchers are mapping the service, KPIs, and scenario-based testing and rehearsal, although this research's aspects again fix the imperatives and encapsulate a broader view of those aspects. Therefore, it also enables organisations to involve more essential considerations in this phase than the matrix of Linkov et al. (2013-b).

The most prominent observation and difference with the resilience matrix of Linkov et al. (2013-b) in this phase is the crisis plan. Linkov and colleagues' (2013-b) matrix advised organisations to establish decision-making protocols in the recovery phase. This research urges to disregard that device because it would be a little too late if the organisation starts thinking about this far in the process.

The consideration that a DDoS can act as a smokescreen and distract the response team from another kind of attack or infiltration is an exciting finding in the absorption phase. This means that the organisation should keep in mind that it should not just focus on the DDoS attack. Besides, this research reasonably follows Linkov et al. (2013-b) aspects but fixed the imperatives again.

In the recovery phase, this research suggested not only reviewing the failures like Linkov and colleagues (2013-b) but the plan and procedures as a whole. Besides that, it also pointed to involve the reputation and the impact on it in this phase.

Instead of determining the motive of the attack, this research suggested providing a rough indication of the attacker's type. Determining the motive would be very challenging and adds little to the organisation's resilience, so this research does not include that in the cognitive domain's adaptation phase.

Moreover, this research also emphasised the depreciation of the plans and provided more room for adjustments, while the paper of Linkov and colleagues (2013-b) only suggested reviewing the plans.

Table 8: Aspects of the cognitive domain

	Plan/prepare	*Absorb*	*Recover*	*Adapt*
Cognitive domain	Mapping of the service	Determination of attack	Review of the plans and procedures	Depreciation of response plans
	KPIs	Decision-making protocols	Reputation	Potential adjustment in plan and procedures
	Crisis plan	Following the plan		Tracking of incidents and impacts
	Scenario-based testing and rehearsal	Determination of whether the attack is over		Rough indication on the attacker's type
		DDoS as a smokescreen		

3.4 The Social domain

In Linkov and colleagues (2013-b: 473), the social domain covers the *'Organisation's structure and communication for making cognitive decisions'*. Next, this research describes the responses of the respondents over the different phases in this domain.

3.4.1 Planning/preparation phase in the social domain

Linkov and colleagues (2013-b: 474) suggest to *'identify and coordinate with external entities that may influence or be influenced by internal cyberattacks (establish point of contact)'*, *'educate/train employees about resilience and organisation's resilience plan'*, *'delegate all assets and services to particular employees'*, *'prepare/establish resilience communications'*, and *'establish a cyber-aware culture'* in this phase of the social domain.

The respondents argued in favour of a Monitoring department, a Mitigation department, a Threat intelligence department, Training, a Division of tasks, an Organisation-wide knowledge of the resilience plan, Outsourcing to CDN service providers, Collaborations, an Understanding of which parties will suffer as a consequence of an attack, and Communication lines in this phase.

The first aspect is a department who handles the detection mechanisms described in the physical domain (Niemantsverdriet). This group or department will monitor the devices and checks the organisation's system. At the Rabobank, there is a team monitoring 24/7. The employees work in shifts, and some people are on standby (Van der Kraan). The response time is usually a little bit longer when an attack happens at night. The organisation has to determine the losses resulting from an attack at different times during the day and night. This determination is specified in the preparation phase of the cognitive domain. This could affect the employees' occupancy because if an online store does not sell products at night, an attack at night will have less impact. It would then make no sense to dedicate much personnel to monitor the servers during the nightly hours.

Not surprisingly, a team or designated person should handle the first mitigation steps when an attack happens. So, the organisation will need a response team (Niemantsverdriet). The organisation sets up this team in the preparation phase to come into action during the absorption phase. Fox-IT also argues for identifying those people who are responsible for enacting and maintaining the incident response plan (Fox-IT, 2020).

Thirdly, a threat intelligence team will keep the organisation ahead on development in the threat landscape (Schaapman, Marshall, De Busser). This would be an R&D department trying to find new techniques and improvements (Schaapman). In the information domain, this research discussed the need to keep up with developments. In this pursuit, the team will follow scientific research and media (De Busser).

Moreover, the larger companies and organisations have a cybersecurity group and a CISO. They would be responsible for mitigating DDoS attacks (Pras). Organisations could also decide to put some people specifically on the mitigation of DDoS attacks. It all depends on the size of the organisation and the number of people available (Pras). In the three aspects above, this research considers them as teams. However, especially the smaller organisations could have only one person for detection, mitigation, and threat intelligence. As this is likely for many organisations, this research will consider the aspects by questioning whether there is someone for the tasks.

Furthermore, this research considers organisations with having one or more persons responsible for the tasks to be more resilient as they would have more time and opportunities to specialise. Likewise, this research will consider an organisation with more people in the teams to be more resilient to DDoS attack. Although the surplus of having more people in the teams is likely to decrease as the team's total number increases, this research will simplify this phenomenon. When and to what degree the surplus will decrease will depend on aspects like the experience of the people involved, the communication within the team, and the time and effort available. Therefore, it will be too complex to consider all of those in this research.

The fourth, fifth, and sixth aspect are to train and educate the people in the teams or departments mentioned above (Marshall, Pras, Hesselman), a division of tasks, and education and training. Training is critical as the way criminals get their foot in the door, is by infiltrating new people and people who are unaware of vulnerabilities (Marshall). According to Hesselman, you need good people who can maintain an overview.

Unsurprisingly, now the organisation will need a division of the tasks. It needs to be clear which team or individual can make decisions at what moment (Niemantsverdriet). This

is the social aspect of the plan and procedures from the cognitive domain. Also, the organisation will have to divide the tasks within a team. Often, managers want to get involved and want to have a continuous understanding of how far the mitigation is progressing and whether the problem has been resolved (Van der Kraan). This involvement slows down the mitigation process.

Comparable to '*educate/train employees about resilience and organisation's resilience plan'* provided by Linkov and colleagues (2013-b), De Busser specifically mentioned *'It is, of course, crucial that everyone in the organisation from the receptionist to the CEO is aware of who is about what when things go wrong.'* Also, Marshall argued for a collective security mindset to protect the whole organisation. Hesselman also discussed this organisation-wide knowledge about DDoS attacks and the importance of it. He addressed the knowledge gap between the technical and legal employees, especially in larger companies. The technical people know precisely how an attack works but the legal people do not (Hesselman). Lawyers have, in essence, risk-averse behaviour. So, if they do not understand something completely, they will act conservatively. Then, it would, for example, become harder to agree to share data about a specific DDoS attack and that, in turn, affects others (Hesselman). A useful link between these groups prevents such inconveniences.

Marshall advised pushing the security to the people who care most, like the developers, the product owner, and the service owner, not the internal security infrastructure department. The organisation could measure how compliant each team is and find out where the gaps are. Then, *'the security department can focus on cool things that they are hired to do, like threat hunting, threat intelligence work, and working at a holistic view to make things better'* (Marshall). This research also includes this aspect of the framework.

Moreover, if there is no support at the management level, there will not be a sufficient budget, not enough people, or expertise (Hesselman). So, the organisation needs awareness at the management level, to enable the right facilities and tools (Hesselman).

The seventh aspect is the outsourcing to CDN service providers (Niemantsverdriet, Schaapman, Pras, Marshall, Hesselman). This research already discussed the doubt whether organisations are even capable of mitigating DDoS attacks themselves in the preparation phase of the physical domain (Niemantsverdriet, Pras, Marshall, and Hesselman). Therefore, an organisation is likely to outsource the mitigation to another party, such as a CDN service provider, at some size of DDoS attack. Those providers aim to provide availability and performance by distributing the service spatially relative to end-users with a geographically

distributed network of proxy servers and data centres. With this network, those providers have different mitigation processes to cover DDoS attacks. This appears to be the solution to the DDoS problem.

Outsourcing the mitigation to those companies also has indirect benefits (Marshall). If the organisation chooses a reputable provider known amongst hackers for protecting well, the hacker can decide to continue and try to overwhelm that provider or move on to the next victim who has a weaker service provider. Comparable, if the organisation has no or an inadequate provider, then they are more likely to be attacked with a DDoS attack (Marshall).

In their study, You et al. (2020) suggested auctions to enable market efficiency and agility with direct pricing based on the real-time supply-demand. In this way, CDN service providers will bid to mitigate DDoS attacks and organisations can incur the winning one. Yang, Lui, Yang, and Wang (2018) provided a trading system for DDoS mitigation services based on blockchain. According to their study (2018: 1036), they have built a *'trust infrastructure, which helps the victim network to set up trust relationships with the remote providers, and enables fast online trading between them to start DDoS mitigation as soon as possible'*. This system includes a credit system to evaluate the credibility of participants.

Another study examined the investment and management of resources (Yuan et al., 2020). The researchers proposed a mechanism that adaptively selects the optimal resource leasing mode for cloud service customers so that they can repel DDoS attacks at minimal financial costs. Their results show that can save 53.58% on average and up to 93.75% on the defence's cost (Yuan et al., 2020).

It is essential to have trust, communication, and clear expectations with the CDN service provider (Marshall). The service provider needs to know what the organisation wants from them and vice versa. *'Bad preparation on your process and your runbooks with a service provider for anti-DDoS will result in as much as a failure as not having a service provider at all'* Marshall said. Organisations can buy off-the-shelf services that will do everything for them, but a whole relationship needs to be managed there.

For small, medium, and large Internet and VoIP (Voice over Internet Protocol) providers, the NBIP (Nationale Beheersorganisatie Internet Providers) offers the NaWas (Nationale Wasstraat) (NBIP, n.d.-a) (Schaapman, Pras). The NBIP is an independent not-for-profit organisation combating DDoS attacks and provides wiretapping services enabling the providers to comply with the Dutch Telecommunications Act (NBIP, n.d.-b). At the NaWas, *'traffic from an attacked provider is routed past our equipment for a thorough "scrub", after*

which the provider receives the clean traffic back over a separate VLAN.' (NBIP, n.d.-a). To be eligible for the service, the organisation must have an AS (Autonomous System) number and be reachable via multiple internet routes (Schaapman). The service is, therefore, not intended for consumers or arbitrary companies. As discussed in the cognitive domain, new participants will get an intake assessment and a DDoS test. Therewith, the organisation and the NBIP will know what to expect from each other.

However, during the interviews, some concerns regarding CDN service providers and the NaWas arose, and it is essential to discuss them here. Firstly, the scrubbing service provider needs to be trusted as the traffic will be routed through its systems. Some organisations want to do their DDoS mitigation themselves because they cannot let any other organisation be able to analyse the traffic (Schaapman).

Even more, if the traffic is routed through a network located in another country, there are different privacy regulations in force. The crisis then transcends political domains (Backman, 2020). The organisation will have to consider whether that is desirable. Especially with critical infrastructures such as banks, Schiphol, and the electricity network, Hesselman would advise keeping that within the European Union and Switzerland. According to him, an organisation could still decide to outsource its DDoS service to companies from America or China, but then the organisation must have the capabilities to oversee its effects. The organisation needs to understand this goes further than just the impact on its business operations because the Internet has become a principal social instrument, and its decision can have effects elsewhere (Hesselman). Moreover, Schaapman even called it quite unimaginable that in Europe and the Netherlands people attach great importance to the GDPR, while, at the same time, companies are rerouting their traffic to American parties.

Another consideration is that when the traffic travels through the third party's systems, the traffic no longer gets to the servers of the organisation (Schaapman). Therefore, it is no longer possible to see what happens. The organisation will not be able to get the information, learn from it, and share it with others (Hesselman). On the other hand, it is possible to make agreements on this. The NBIP, for example, always provides a report of the DDoS attack which describes the size and the DDoS types of the attack (Schaapman).

Eighthly, in the Netherlands, there are some collaborations to fight DDoS attacks (Niemantsverdriet), for example, the Nationale Anti-DDoS-coalitie (National Anti-DDoS-Coalition) No More DDoS (Pras). This collaboration consists of seventeen organisations including governments, internet providers, internet exchanges, academic institutions, non-

profit organisations and banks (No More DDoS, n.d.). The anti-DDoS coalition has set up six working groups, each dealing with one theme surrounding DDoS attacks (NCSC, n.d.-b). Those are Legal Affairs, Communication, Clearinghouse, Practice, Cross-sector collaboration, Basic agreements and measures (NCSC, n.d.-b). There are specialists from different organisations in each working group. According to Hesselman, if an organisation wants to solve DDoS attacks on the Internet, it will have to work together with others. The Internet is one colossal collaboration; it consists of 70,000 different networks (Hesselman). That is a missing component in the current matrix. Therefore, this research will include collaborations as an aspect of this domain.

Of those working groups, the working group Clearinghouse is committed to measuring DDoS attacks' technical characteristics via so-called DDoS fingerprints to exchange this information between participants (NCSC, n.d.-b). This research already covered the DDoS fingerprints in the preparation phase of the physical domain. Participants of the coalition can share the fingerprints, and others can anticipate it. Thus, when a DDoS attack comes in at another participant, the organisation can immediately recognise the attack and take necessary measures.

Another example is the working group Practice. That working group aims to practise with DDoS attacks and enables coalition members to learn from them (NCSC, n.d.-b). In the anti-DDoS-coalition, the participants practice with mitigating DDoS attacks (Pras). This is done in red and blue teaming; one participant attacks another participant, which tries to mitigate the attack (Pras). Being committed to collaboration would enable the organisation to practise and test DDoS attacks on its systems.

An organisation could also consider collaborating with competitors within its industry (Niemantsverdriet, Marshall). According to Marshall, there is a very socially-contiguous business environment. Different businesses, especially around security, share their approaches, knowledge, and information (Marshall). Collaboration within an industry depends on the specific industry and how intense the organisation wants to work with its competitors (Niemantsverdriet). This kind of collaboration has its benefits.

For example, the Dutch banks have mutually agreed to share information about attacks when those come in (Van der Kraan). On cybersecurity, banks are not competitors but share their infrastructure to have a lot more capacity than if they were to do it all by themselves (Pras, Van der Kraan). It has already occurred that as one bank was attacked, other banks could adjust

their systems. Thereafter, the attackers shifted their aim without success as the other banks had anticipated it (Van der Kraan).

Thus, an organisation participating in collaboration is likely to be more resilient to DDoS attacks. Therefore, this research considers collaboration as an aspect of this phase. In a partnership, it is possible to share information and knowledge (Hesselman, Pras) and train together for DDoS attacks (Pras). Likely, a single organisation is no longer able to mitigate a DDoS attack. Therefore, besides sharing information and training, organisations could also collaborate in mitigating DDoS attacks.

Other factors that should be considered are the affected parties and communications lines. The organisation will also need to understand which parties will suffer when the organisation's system goes down due to a DDoS attack (Niemantsverdriet). Most of the time, those will be customers. The organisation would like to inform those parties and avoid professional jargon.

A result of the DDoS attack is that communication lines could be down as well (Niemantsverdriet). The organisation will have to figure out how it will communicate with its employees and teams, its customers, its CDN service provider, its collaborators, law enforcement, and all other parties involved. In some cases, it would also be wise to consider a second and third line of communication to make sure the organisation can receive and share information. Usually, organisations use social media like Twitter to inform customers that its systems are down due to a DDoS attack (Schaapman).

Besides, one respondent specifically argued that people in the security departments already are cyber-aware; otherwise, they would not work in that position (Van der Kraan). Cyber-awareness is more about phishing emails and setting up strong passwords, but this does not really have to do with DDoS. This research already covered the organisation-wide understanding of the resilience plan. This resilience plan-awareness, so to say, is a specific part of the broader cyber-awareness. This research will not include the need for a cyber-aware culture but addresses the employees' understanding of the resilience plan.

3.4.2 Absorption phase in the social domain

Linkov and colleagues (2013-b: 474) indicate to *'locate and contact identified experts and resilience responsible personnel'* in the absorption phase of the social domain.

In this research, the respondents argued in favour of the Detection of the attack and initiation of the mitigation process, Notification of customers, Notification of authorities, a File of the report, and a Commitment to the division of tasks or a response team in this phase.

The first aspect is whether the detection department actually detects the attacks during this phase (Niemantsverdriet). In the preparation phase of this domain, the organisation has set up a department. Thereafter, this department needs to activate the mitigation department and start their response (De Busser). This aspect is comparable to the task of coordination of Boin et al. (2005). This includes coordinating actions and actors involved. Therefore, this research includes whether this department accomplished this task.

Secondly, the organisation wants to let customers know it is mitigating a DDoS attack (Niemantsverdriet, Marshall, Pras). In a more general sense, Boin et al. (2017: 79) argued that the task of meaning-making and communication includes formulating *'a comprehensive account of what is going on and distribute it successfully to affected audiences, involved actors and stakeholders'*. In the preparation phase, this research laid out the understanding of the parties that will suffer from a DDoS attack on the organisation's systems. Niemantsverdriet questioned: *'What would we like our customers or users to see or experience when we are repelling an attack'*. Therefore, this research includes the aspect of whether suffering parties get a notification of the attack.

Furthermore, the organisation must notify several authorities as soon as there is a DDoS attack or as soon as there is customer impact (Van der Kraan). Figuring out which authorities need to be notified is challenging as it turned out those authorities themselves know they want to be informed but how and when is still rather vague (Van der Kraan). In case the organisation is a bank, the organisation should probably quickly notify the Nederlandse Bank and the NCSC (Pras). Besides, in some cases, it will be wise to inform the media before they start writing about the organisation and the attack without the organisation's side of the story (Pras). The organisation will need to have someone or a team arranging public relations.

Unsurprisingly, it is also essential to file a report (Pras). Then, Team High Tech Crime of the Dutch police will start their investigation. In particular, that team and the FBI, Interpol, and Europol, regularly pick up the people who run booter sites (Pras). Team High Tech Crime is also directly involved in the Clearing House working group of the anti-DDoS coalition (Schaapman). There are regional offices and a specific group that is engaged in taking down botnets. They try to collect as much information as possible of the botnets and try to find the command and control server (Schaapman). The work of Kopp et al. (2019) examined the

effectiveness of the FBI's takedown of fifteen booter websites in 2018. They concluded that it led to a temporary reduction in attack traffic. One booter was able to continue its operations by using a new domain for its website (Kopp et al., 2019). Collier, Thomas, Clayton, and Hutchings (2019) found the same effect and saw that the operation reduced the DDoS attacks by a third for at least ten weeks and resulted in a lasting change to the structure of the booter market.

During the attack, the organisation would like to keep the technical employees working on the issue and not disturbed by management or the legal department. This is the next aspect in this phase. This has all to do with the division of tasks and the organisation-wide understanding of the resilience plan from the preparation phase of this domain. On the other hand, the organisation could also decide to appoint a DDoS response team (Van der Kraan). That team could be a composition of technical, managing, legal, and communication staff. With such a team, the organisation could overcome possible knowledge gaps between those kinds of employees. The organisation can also appoint a coordinator, who keeps the oversight and correspondents with the different departments (Van der Kraan).

3.4.3 Recovery phase in the social domain

'Follow resilience communications plan' and *'determine liability for the organisation'* are two aspects to consider when in the recovery phase in the social domain (Linkov et al., 2013-b: 474).

The respondents of this research came to a Notification of authorities, Acquisition of insurance, Determination of liability, and an Incorporation of legal implications of outsourcing to CDN service providers.

The first aspect of this phase is comparable to the third aspect of the previous phase. The organisation also wants to inform authorities when it is recovering from the attack. More information will be available to the organisation and authorities, and other external organisations will use this (Niemantsverdriet).

Niemantsverdriet thinks there is often a tendency to keep the cards close to the chest. Organisations do not want to tell something is going on and are likely to remain mysterious. The risk is that if the news will eventually go out, the organisation is in a weaker position than when it was open about it from the start (Niemantsverdriet). It may be culturally determined as the Netherlands tends to be a bit more transparent than other countries in Europe.

In general, it is hard to deny there has been an attack; everyone can see that. However, whether it was dealt with cleverly or not is more comfortable to keep in the ambiguous. Sometimes, an attack comes at a very inconvenient time and, therefore, some things go wrong that usually would not be the case.

The closed nature is not only attributable to organisations. Somehow, society tends to rely on a kind of victim-blaming (Niemantsverdriet). As soon as a company is hacked, we tend to look for it not having its systems in order or the patches not entirely up to date.

The next two aspects are the acquisition of insurance and determine liability for the organisation. There are many different insurances available such as against failure of cloud suppliers' computer equipment (Schaapman). There are also insurances to cover the losses due to a DDoS attack.

De Busser specifically shared her concerns with the aspect *'determine liability for the organisation'* of Linkov and colleagues (2013-b: 474). In her opinion, this would better fit into a legal domain instead of social. Here, lawyers need to know what kind of damage claims to expect. On the other hand, she did not question the importance of this aspect.

Moreover, the outsourcing to CDN service providers also has legal implications (Hesselman). This research already addressed these implications in the preparation phase of the social domain. But to discuss them briefly, if the network traffic is directed to servers in the U.S. or China, the organisation will be involved in those countries' jurisdictions.

3.4.4 Adaptation phase in the social domain

In this last phase of the social domain, measuring the resilience to cyberattacks lays in *'evaluate employees response to event in order to determine preparedness and communications effectiveness'*, *'assign employees to critical areas that were previously overlooked'*, and *'stay informed about latest threats and state of the art protection methods/share with organisation'* according to Linkov and colleagues (2013-b: 474).

In this research, the respondents suggested a Culture open to improvements, an R&D department, Evaluation of employees and their procedures, Evaluation of external parties, Evaluation of communication, and an Assignment of employees to overlooked areas.

The first aspect is to create a culture open to improvements. The organisation has to consider the importance of smaller incidents (Niemantsverdriet). Sometimes in factories, people place giant banners stating how many days the factory was running without an incident. This may create a culture in which people might be scared to report something small.

For example, if an employee drops a hammer on his feet, he will think twice before reporting it and get that excellent score off the board or not receiving a bonus while there could be something wrong that shows a deeper underlying problem (Niemantsverdriet, De Busser). But not reporting the smaller incident, something else but similar might happen which could seriously injure someone. That is a trade-off where fewer incidents is not necessarily better (Niemantsverdriet). Niemantsverdriet also thinks it is unnecessary to strive for an absolute value but rather to find a kind of trend line that goes up or down.

Therefore, the organisation will have to create a culture which advocates improvements and development. When there are aspects in the detection and mitigation of DDoS attacks in need of improvement and the organisation decides to commit to improvement, Van der Kraan advised improving by using the systematic approach KAIZEN. This approach is primarily based on continuous improvement and building a culture where all employees, from plant floor employees to the CEO, actively suggest and implement improvements (Lean Production, n.d.). Another idea would be to enable anonymous reports, although this would be challenging in smaller organisations (De Busser).

Another aspect is that the organisation needs a person or team to make sure all relevant information is on the table and determine what went wrong or what could have gone better during the attack (Van der Kraan, De Busser, Marshall, Pras). Based on this information, the organisation will know where to improve and can determine what improvements it will make. This decision could very well be financially dependent.

When the organisation is outsourcing to CDN service providers, the organisation is less likely to get all the information (Schaapman). It is the providers' unique selling point to mitigate DDoS attacks and provide knowledge about the organisation could potentially harm their business model.

Unsurprisingly, the evaluation has also got a social component (Van der Kraan, De Busser). The organisation has to evaluate whether the employees are following procedures and improving those procedures. Who responded at what moment and could this be done faster? (Niemantsverdriet). Pras questioned: Did the employees stick to the guidelines? And if not, did they have a good reason to deviate from that or not?

Although the evaluation of procedures is primarily covered in the Adaptation phase of the cognitive domain, it is essential to note that the organisation needs to handle the assessment of employees thoughtfully as a severe consequence for mistakes by employees will contribute

to a closed culture in which employees are likely to keep minor incidents to themselves (Niemantsverdriet).

To build up on the aspects of outsourcing from the planning and preparing phase, if the organisation outsources a part of the mitigation to an external party, the organisation will have to decide whether external parties follow the right procedures and whether they provide good services (Van der Kraan, Pras; Fox-IT, 2020). If the organisation has received insufficient help from protecting parties, it will cover this shortcoming.

The fifth aspect is to determine whether the communication was effective (Van der Kraan). Different teams and external parties may have acted excellently. However, it could very well be that the communication between the parties went badly and that errors arose as a result.

In line with the aspect of Linkov and colleagues (2013-b: 474) *'assign employees to critical areas that were previously overlooked'*, Van der Kraan also argued in favour of such an aspect. For example, if the communication with a third party was overlooked, then the organisation will put this more prominently in the procedures. Marshall added that the organisation should look at what was overlooked and at the cause and what was attacked. The organisation should also think in different roles and bring in a workshop team and have a task force for a few months to try and solve eighty per cent of the problems it finds and put twenty per cent back to a more steady-state improvement (Marshall). This research would, therefore, include an assignment of employees to overlooked areas.

3.4.5 Conclusions on the social domain

The previous sections suggested twenty-five aspects of the social domain. The results proposed aspects in all phases and table 9 shows the aspects over the different phases.

The number of aspects in the planning and preparing phase of this domain is remarkably high. This research's findings put much more emphasis on the social domain than Linkov and colleagues (2013-b). It became evident that there is a lot to do in this part of the matrix: setting up different departments, divide functions, and managing relationships with other parties are some of them.

Comparable to Linkov and colleagues (2013-b) model, this research also suggested to initiate the mitigation process in the absorption phase. Decisive differences, however, are the notifications to customers and authorities. This research involved more external

communication and ensuring the informing customers and authorities than Linkov and colleagues (2013-b) did.

This research included the organisation's liability and the legal implications of outsourcing to CDN service providers in the recovery phase. Furthermore, it is also possible to take out insurance and this research involved that unlike Linkov and colleagues (2013-b).

Besides the assignment of employees to overlooked areas and evaluations of employees, this research suggested that external parties' evaluation and communication are also essential for resilience. Moreover, compared to the matrix of Linkov et al. (2013-b), this research also emphasised improvement by including a culture open to improvements and an R&D department.

Remarkably, this research did not include an aspect comparable to the *'stay informed about the latest threats and state of the art protection methods/share with the organisation'* of Linkov and colleagues (2013-b). This aspect's position by those researchers is rather odd, and this research covered its essence in the information domain.

Table 9: Aspects of the social domain

	Plan/prepare	*Absorb*	*Recover*	*Adapt*
Social domain	Monitoring department	Detection and initiation of mitigation	Notification of authorities	Culture open to improvements
	Mitigation department	Notification of customers	Acquisition of insurance	R&D department
	Threat intelligence department	Notification of authorities	Determination of liability	Evaluation of employees and their procedures
	Training	File of the report	Incorporation of legal implications of outsourcing	Evaluation of external parties
	Division of tasks	Commitment to division of tasks or response team		Evaluation of communication
	Organisation-wide knowledge of the resilience plan			Assignment of employees to overlooked areas
	Outsourcing to CDN service providers			
	Collaborations			
	Understanding of parties involved			
	Communication lines			

4. Rethinking the resilience matrix

This chapters lays the foundation for a new model to cover the flaws of Linkov et al. (2013-b) resilience matrix. Subsequently, this section will discuss the suggestions by respondents and provide concrete insights on resilience measures.

4.1 Suggestions by respondents

In several occasions, the current matrix of Linkov and colleagues (2013-b) was not adequate. This made it difficult for the respondents to name and classify factors in a specific place in the matrix. This chapter will discuss these problems and works towards a new matrix.

In a general sense, the respondents suggested that the preparation phase remains somewhat underexposed (Niemantsverdriet). In many cases, the matrix suggests that the organisation only starts thinking about essential elements for DDoS mitigation when they are in the middle of absorbing and recovery. Normally, this is too late. Niemantsverdriet specifically advised starting thinking about DDoS attacks as much as possible before it happens. To Marshall, it seemed as though companies would start to plan and prepare after they had suffered their first attack. If an organisation would operate in this way, it is always reactive. Moreover, De Busser specifically addressed the *'establish decision-making protocols or aids to select recovery options'* of Linkov and colleagues (2013-b) in the recovery domain. It would not make sense to establish these protocols at the moment when the organisation needs them. Those protocols should already be in place before an attack happens. Also, Hesselman added that he thinks that if the organisation prepares, handles, and accommodates in the earlier phases, then the organisation does not have to do much more in the later phases. In line with the suggestions of the respondents, this research would also suggest putting more emphasis on the preparation phase.

Therefore, the first adjustment of the matrix is that an organisation should implement all aspects and considerations in the preparation phase in the matrix. This changes the approach of the matrix drastically as an organisation will be required to think about all of the considerations before an attack. Another consequence is that the other phases are only applicable during or after an attack or test. As a result, the matrix will consider the aspects of those phases in the preparation phase.

Secondly, the third and fourth phases are not strictly delineated and seem to intertwine (Niemantsverdriet). Linkov and colleagues (2013-b: 474) defined those phases as: *'restore all asset function and service availability to their pre-event functionality´* and *'using knowledge*

from the event, alter protocol, configuration of the system, personnel training, or other aspects to become more resilient'. However, the recovery phase has got to *'establish decision making protocols or aids to select recovery plan'* and uses the term *'review'* in some of the aspects. Therefore, the Linkov and colleagues cause ambiguity because it seems as mentioned aspects should be in the Adaptation phase. In rethinking the matrix, this research will prevent this.

Thirdly, De Busser also argued in favour of a new domain: the legal domain. Especially the positioning of Linkov and colleagues' (2013-b) *'determine liability for the organisation'* in the recovery phase of the social domain is rather strange. De Busser suggested to put this aspect in a domain of lawyers who need to know what kind of damage claims the organisation could expect in certain situations. Pras could also imagine some people will find the legal perspective interesting.

Now, the model considers this very generally with liability, but it depends on what a DDoS exactly causes (De Busser). For example, it can make equipment or data inaccessible. Those are very different scenarios as in the former, the organisation could expect damage claims, but with the latter, it is also about data protection and privacy, and those claims could be much higher. De Busser suggested adding a lawyer to the crisis management team to map out the legal consequences.

The literature review shows that there is little research done into DDoS attacks in a legal context. Also, the study of Nikolskaya and Minbaleev (2020) stated that legal regulation of incidents related to DDoS attacks is a new area. On the other hand, the research of Singh and Sharma (2019) addressed this. They examined the threats of DDoS attacks and reviewed Indian law. In doing so, they revealed various issues and concerns (Singh & Sharma, 2019).

Another interesting study is that of Watkins, Silberberg, Morales, and Robinson (2015). Those researchers examined the threat posed by a family of DDoS toolkits, an overview of the hacking back debate and legal loopholes or implied immunity, and novel offensive campaigns stopping DDoS attacks by exploiting vulnerabilities in the botnets.

Fourthly, this study argues for splitting up the social domain into internal and external matters. Although it is not immediately apparent from the interviews, and respondents did not directly indicate this, those are two different relationships that the organisation will have to maintain. For example, the organisation will communicate completely different with its employees (internal) compared to its competitors (external).

4.2 Measurements of resilience

A lot of elements are involved in measuring an organisation's resilience. Although this research does not specifically address how the aspects should be measured, it is compelling to mention insights from this research especially as the resilience matrix of Linkov et al. (2013-b) was insufficient on this point.

4.2.1 Overall system resilience

Linkov & Trump (2019) and Ganin et al. (2016) suggest two approaches for measuring resilience. The resilience matrix is the semi-quantitative approach and the researchers use Network Science for a quantitative approach. For assessing the resilience with the former method, the sixteen cells of the matrix each get a value that summarises the scope of the system to perform within that domain and period of time (Linkov & Trump, 2019). Then, Fox-Lent et al. (2015) recommended (Linkov & Trump, 2019: 88):

1. *'to clearly outline the system or project's boundaries along with an array of hazard and threat scenarios that could impact the system,'*
2. *'to enumerate critical system functions and capabilities that must be upheld and maintained throughout a crisis or shock,'*
3. *'to select indicators for each critical function and subsequently compute performance scores in each matrix cell, and'*
4. *'[to] aggregate all cells of the matrix - if necessary - to provide an overall system resilience rating, informing on the system's ability to respond to and overcome from external shock.'*

Linkov and Trump (2019) argued that in the best case, the research should bring together a group of representatives from the community such as municipal representatives from emergency management, community development, and local threat management. In the case of DDoS resilience, the research should involve crucial employees in DDoS mitigation and management.

If the organisation would choose to add relative importance of each matrix cell, the measurement should include criteria weights for the aggregation to an overall system resilience rating. An example can be taken of the research of Ganin et al. (2017), which constructed a multicriteria decision framework for cybersecurity. The weights will differ and are the result of predetermined management needs, perceptions, and goals (Linkov & Trump, 2019).

To measure specific aspects in the matrix, this research is inspired by the paper of Sikula, Mancillas, Linkov, and McDonagh (2015). These researchers propose a scoring system assessing elements with a score from one to seven.

Although it is beyond the scope of this research to come up with a specific methodology for measuring the aspects in the matrix, the text above provided an indication on the steps forward. It mainly functioned as a check whether the proposed aspects should come to a resilience measure.

Between the aspects and cells, there are interrelationships (Niemantsverdriet, Van der Kraan, Marshall). The main shortcoming of this the approach illustrated above is the lack of calculations on those interrelationships. For example, if an organisation would choose to invest in the best automatic monitoring, detection, and mitigation system, it would not make sense also to hire an extensive number of employees monitoring the systems for DDoS attacks. In the matrix, however, implementing both would increase resilience. Frankly, the researches Linkov et al. (2013-b), Linkov & Trump (2019), and Ganin et al. (2017) did not address this vital insight.

4.2.2 Testing and incidents as the main drivers for resilience measurements

Marshall disagreed with the significance of the adaptation phase. In his opinion, it should actually be replaced with continuous improvement rather than something that happens because of an event; it should happen all the time. For this reason, the organisation will have to go through the phases of the matrix while testing its system and when attacks happen on other organisations' systems.

As discussed in the cognitive domain, measuring resilience with fictive cases would only be valid to an extent. The organisation would only know its resilience with the most realistic tests or actual attacks. Since the main reason for resilience measuring is being prepared for potentially disastrous events, this research urges organisations to invest in testing.

4.2.3 Resilience matrix intervals

Marshall argued that measuring cyber resilience is not something that is a static measurement. Over the course of weeks, months, or even years, the measurement becomes less and less relevant. If the organisation measures its resilience every month, the organisation could still be falling behind. The less the organisation has an adaptive approach where it keeps looking for new ways to improve its service, the worse the resilience is over time (Niemantsverdriet,

Marshall). Linkov & Trump (2019) also argued updating the matrix at regular intervals because the resilience matrix does not intrinsically capture the various temporal characteristics that could cause shifts in preferences or needs over time. Therefore, this research advocates that organisations would need to keep measuring their resilience over time and depreciate the validity of measurement as time passes.

5. Conclusion

As the threat of DDoS attacks is on the rise, organisations will have to evoke their defence mechanisms and wake up its guardians. Scholars have made a tremendous effort to contain the notion of security. However, this research showed that resilience could provide a much better and more concrete insight to indicate the weathering and averting of DDoS attacks.

The research examined previous efforts to grasp resilience and found the resilience matrix of Linkov and colleagues (2013-b). Unfortunately, the matrix was not specific to DDoS attacks, insufficient, vague, and the aspects turned out to be unmeasurable. Other research showed that the matrix was flexible enough to be applied on different topics. This prompted the research into questioning which aspects would be vital to measure resilience against DDoS attacks.

To answer this inquiry, this research consisted of expert interviews and a systematic literature review. The research found elements in the different domains and phases and suggested 68 aspects for the DDoS resilience matrix. By rethinking the matrix, the research substantiated to make adjustments to the matrix, examined resilience calculations, and addressed the necessity of testing and intervals.

This research showed factors for measuring cyber resilience. In every phase of every domain, the research discovered aspects. Together with the insights on measuring resilience, this research provided a step to measurable resilience to DDoS attacks. Table 10 displays the DDoS resilience matrix with the updated aspects and adjustments.

Table 10: DDoS Resilience Matrix

	Plan/prepare	*Absorb*	*Recover*	*Adapt*
Physical domain	Mapping on the network structure	Working mitigation and detection systems	Assessment of service/asset damage	Review of assets and service configuration
	Mitigation systems	Sufficient separation	Reparation or replacement of damaged assets	Phase-out of obsolete and introduction of new assets
	Detection systems	Tracker of the response time	Reparation or replacement of malfunctioning systems	
	Separation of the network		System to measure the recovery time	
			Required functionality	
Information domain	Locations to store DDoS data	Signal	Securing log files	Debriefing
	Separation of data storage	Capacity to store and log files	Standards in CTI language and exchange	Information to adopt
	Sharing possibilities	Informing authorities and relevant vendors		Information share with partners
	Retrieving possibilities	Real-time monitor		Addition of intelligence
	Standardised storing and sharing	Threshold for valid information		
	Profile of normal traffic			
	Access rights			
	Encryption			
Cognitive domain	Mapping of the service	Determination of attack	Review of the plans and procedures	Depreciation of response plans
	KPIs	Decision-making protocols	Reputation	Potential adjustment in plan and procedures
	Crisis plan	Following the plan		Tracking of incidents and impacts
	Scenario-based testing and rehearsal	Determination of whether the attack is over		Rough indication on the attacker's type
		DDoS as a smokescreen		
Internal domain	Monitoring department	Detection and initiation of mitigation process	*	Culture open to improvements
	Mitigation department	Commitment to the division of tasks		R&D department
	Threat intelligence department			Evaluation of employees and responses
	Training			Assignment of employees to overlooked areas
	Division of tasks			
	Organisation-wide knowledge of the plan			
External domain	Outsourcing to CDN service providers	Notification of customers	Notification of authorities	Evaluation of external parties
	Collaborations	Notification of authorities	Acquisition of insurance	Evaluation of communication
	Understanding of parties involved	File of the report		
	Communication lines			
Legal domain	*	*	Determination of liability	*
			Incorporating legal implications of outsourcing	

*: not covered in this research

6. Discussion

This chapter addresses the discussion on the research. Consecutively, it indicates the research's validity, interprets the results, discusses the limitations and implications, and provides future research suggestions.

This research's results show that there are aspects of measuring resilience. None of the respondents pointed out that it was not possible to measure resilience based on factors. However, most of them indicated that it would be very challenging in practice to make measurements.

This research also indicates that Linkov et al. (2013-b) 's matrix provides a solid structure to unravel resilience aspects. After all, this research finds 68 aspects for measuring resilience to DDoS attacks. At the same time, the matrix provided enough flexibility to adjust the topic to DDoS attacks.

Moreover, the 68 aspects indicate that an organisation could improve its resilience when it improves those aspects. It follows from this research that resilience will increase as the aspects also increase or improve. Quantitative analysis will have to show whether this is the case.

At this point, it seems that organisations could measure their resilience with an even more improved version of the resilience matrix. This improvement would mean that organisations would determine their resilience and weaknesses in the organisation and systems. It follows that organisations could make informed decisions about improving their resilience and do so more efficiently.

In this way, organisations could improve their systems more at the same costs or improve at the same rate at lower prices. Either way, measuring DDoS resilience would enlighten the sketched DDoS dystopia of the introduction.

6.1 Limitations

Although the researcher has set up this research with the best intentions and has gone to extremes to achieve successful analysis, it is necessary to identify the flaws of this study.
The first limitation would be the selection of interviewees. The study failed to enter into dialogue with all stakeholders. The number of respondents is somewhat limited compared to the number of factors involved with the resilience matrix.

For example, it would be interesting to involve ISPs such as KPN, T-Mobile, and Vodafone-Ziggo. According to Van Eeten and Bauer (2008), those companies play a vital role in DDoS mitigation as malicious traffic runs through their networks.

Including a military actor into the research could also lead to new insights. As discussed in the theoretical framework, the resilience matrix initially has a military basis. Therefore, it would be compelling to involve them again.

The third type of interesting actor would be commercial CDN service providers. This research examined and criticised their business. For that reason, it is essential also to highlight their side of the story. For all we know, those companies establish clear and proper agreements about data access, privacy, and regulations concerns.

Moreover, taking a holistic approach to tackle the DDoS problem is challenging and paves the way for the second limitation. It requires the researcher to cover many different disciplines, such as computer science, crisis management, psychology, business management, and law. Although this study involved respondents with various backgrounds, it could benefit from a collaboration of researchers with different expertise.

The final limitation is the inability to address the interrelationships between the matrix's aspects. Although several respondents directly discussed the correlations between aspects, this research was insufficient in examining those relations.

6.2 Future research

One does not have to have a rich imagination come up with the next steps after this research. We could first look at the limitations of this research first and improve the selection of interviewees. Future scholars could conduct a comparative study of this research but involve more respondents, in general, and involve underexposed actors like ISPs, military actors, and CDN service providers.

Another way forward would be to engage scholars with different backgrounds. Since mapping DDoS resilience for organisations would require a holistic approach, different views and expertise will reveal a wide range of opportunities.

Future research could also aim at the interrelations between the aspects and develop a method to take those into the measurement procedure. As stated before, the current matrix would not be able to accommodate this.

The easiest path is to repeat this research every so often. Due to cyberspace's dynamic environment and the creativity of those who go there, new critical aspects with emerge. It would be vital to keep the matrix up-to-date.

Moreover, this research did not aim to offer measurements for the individual aspects but rather to identify them. Future research could tackle this part of DDoS resilience measurement.

If an organisation wants an overall systems resilience rating, scholars will have to grasp an understanding of adding weights to the equation. To do this, they will then have to prioritise certain parts of the system.

Finally, the attentive reader has noticed that this research did not provide many aspects of the new domains: the legal, internal, and external domain. The splitting up and adding of these domains is based on the results of this research, and, therefore, the interviews did not question those domains specifically. Scholars could investigate these domains in the future.

References

1. Accenture (2018). Gaining ground on the cyber attacker: 2018 State of Cyber Resilience. Retrieved on February 29, 2020, from https://www.accenture.com/_acnmedia/pdf-76/accenture-2018-state-of-cyber-resilience.pdf
2. Ahmed, M. E., Ullah, S., & Kim, H. (2019). Statistical Application Fingerprinting for DDoS Attack Mitigation. *IEEE Transactions on Information Forensics and Security*, 14(6), 1471-1484.
3. Akamai (2020). 2020: A year in review, 6(4). Retrieved on December 6, 2020, from http://email.akamai.com/E8H0S4ylKJu080CN2u0f50I
4. Akamai (n.d.-a). DDoS Protection. Retrieved on December 25, 2020, from https://www.akamai.com/us/en/resources/ddos-protection.jsp
5. Akamai (n.d.-b). Can DDoS Attacks Be Stopped in Zero Seconds? Retrieved on January 26, 2021, from https://www.akamai.com/uk/en/multimedia/documents/infographic/can-ddos-attacks-be-stopped-in-zero-seconds.pdf
6. Alharbi, T., Aljuhani, A. & Hang Liu (2017). Holistic DDoS mitigation using NFV, *IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, 1-4. Las Vegas, NV.
7. Almeida, V.A.F., Doneda, D., & De Souza Abreu, J. (2017). Cyberwarfare and Digital Governance. *IEEE Internet Computing*, 21(2), 68-71.
8. April, T., Chapin, L., Claffy, K.C., Hesselman, C., Kaeo, M., Latour, J., McPherson, D., Piscitello, D., Ransmussen, R., and & Seiden, M. (2019). The DNS and the Internet of Things: Opportunities, Risks, and Challenges.
9. Backman, S. (2020). Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management*, 1-10.
10. Baldwin, D.A. (1997). The concept of security. *Review of International Studies*¸ 23, 5-26.
11. Bodeau, D.J., Graubart, R.D., Picciotto, J., & McQuaid, R. (2011, September). Cyber Resiliency Engineering Framework. MITRE. Retrieved on Septempber 12, 2020, from https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework

12. Boin, A., Hart, P.T., Stern, E.K., & Sundelius, B. (2005). *The politics of crisis management: Public leadership under pressure.* Cambridge University Press.
13. Boin, A., Hart, P.T., Stern, E.K., & Sundelius, B. (2017). *The politics of crisis management: Public leadership under pressure*, 2nd ed. Cambridge University Press.
14. Broeders, D., De Busser, E., & Pawlak, P. (2020, April). Three tales of attribution in cyberspace. Retrieved on November 16, 2020, from https://eucyberdirect.eu/content_research/three-tales-of-attribution-in-cyberspace/
15. Capgemini (2017). Trends in Cybersecurity 2017-2018. Retrieved on February 28, 2020, from https://www.capgemini.com/nl-nl/wp-content/uploads/sites/7/2017/11/trends-in-cybersecurity-report-2017-2018.pdf
16. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. Communications of the ACM, 47(7), 87-92.
17. Chadd, A. (2018). DDoS attacks: past, present and future. *Network Security*, 7, 13-14.
18. Collier, B., Thomas, D.R., Clayton, R., & Hutchings, A. (2019). Booting the Booters: Evaluating the Effects of Police Interventions in the market for Denial-of-Service Attacks. *Proceedings of the Internet Measurement Conference*, 50-64.
19. Collier, Z.A., DiMase, D., Walters, S., Tehranipoor, M.M., Lambert, J.H., & Linkov, I. (2014). Cybersecurity Standards: Managing Risk and Creating Resilience. *Computer*, 47(9), 70-76.
20. Cox, L.A. (2009). Game Theory and Risk Analysis. *Risk Analysis*, 29(8), 1062-1068.
21. Das, S., Venugopal, D., & Shiva, S. (2020). A holistic approach for detecting ddos attacks by using ensemble unsupervised machine learning. In *Future of Information and Communication Conference*. 721-738. Springer, Cham.
22. DDoSDB (n.d.). What is DDoSDB? Retrieved from https://ddosdb.org/
23. De Volkskrant (August 16, 2013). DigiD na DDoS-aanval weer beschikbaar. Retrieved at December 12, 2019, from https://www.volkskrant.nl/nieuws-achtergrond/digid-na-ddos-aanval-weer-beschikbaar~b7072db2/
24. Deloitte (2018). Building resilience to denial-of-service attacks. Retrieved at February 28, 2020, from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-building-resilience-to-denial-of-service-attacks.pdf

25. Dijkman, R.M., Sprenkels, B., Peeters, T., & Janssen, A. (2015). Business models for the Internet of Things. *International Journal of Information Management*, 35(6), 672-678.
26. DiMase, D., Collier, Z.A., Heffner, K., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience, *Environment Systems and Decisions*, 35, 291-300.
27. EESC (2018, March). Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks. Retrieved on February 29, 2020, from https://www.thehaguesecuritydelta.com/media/com_hsd/report/191/document/qe-01-18-515-en-n.pdf
28. Eisenberg, D. A., Linkov, I., Park, J., Bates, M., Fox-Lent, C., & Seager, T. (2014). Resilience metrics: lessons from military doctrines. Solutions, 5(5), 76-87.
29. Fachkha, C, Bou-Harb, E., & Debbabi, M. (2014). Fingerprinting Internet DNS Aplification DDoS Activities. *2014 6th International Conference on New Technologies, Mobility and Security (NTMS)*, Dubai, 1-5.
30. Fenton, N. & Neil, M. (2012). *Risk assessment and decision analysis with Bayesian networks* (1st ed.). CRC Press.
31. Fox-IT (2020). Prepare and Respond: The Guide to Cyber Incident Response Planning. Retrieved on December 10, 2020, from https://resources.fox-it.com/202011-Guide-Cyber-Incident-Response-Planning.html
32. Fox-IT (n.d.). Abusing cloud services to fly under the radar. Retrieved on January 12, 2021, from https://blog.fox-it.com/2021/01/12/abusing-cloud-services-to-fly-under-the-radar/?mkt_tok=eyJpIjoiT1dVMFkySmpOamxrTkRRMiIsInQiOiI5ME1ieGRka2l4cVBtY1VubmlQZVwvaHdNcWdcL2lTMjdxUTIyY0NsNktHdmg1MXVIYmllcmxaY1daUlBrQlVYdm5GMmlpeUozZnZEZWJoQ1lsOHFzSWw0bGNFQVZLcVQ4VkxGbmRNREtaZHFMSEZDWEQ3U2J6TFJYbDc0YUlRXC83OCJ9
33. Fox-Lent, C., & Linkov, I. (2018). Resilience Matrix for Comprehensive Urban Resilience Planning. *Resilience-Oriented Urban Planning*, 29-47.
34. Fox-Lent, C., Bates, M.E., & Linkov, I. (2015). A matrix approach to community resilience assessment: an illustrative case at Rockaway Peninsula. *Environment Systems and Decisions*, 35, 209-218.

35. Ganin, A.A., Massaro, E., Gutfraind A., Steen. N., Keisler, J.M., Kott, A., Mangoubi, R., & Linkov, I. (2016). Operational resilience: concepts, design and analysis. *Scientific Reports*, 6.
36. Ganin, A.A., Quach, P., Panwar, M, Collier, Z.A., Keisler, J.M. Marchese, D., & Linkov, I. (2017). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Analysis*, 40, 183-199.
37. Harrison, T. (2015). Virtuous reality: moral theory and research into cyber-bullying. *Ethics and Information Technology*, 17(4), 275-283.
38. Hesselman, C., Kaeo, M., Chapin, L., Claffy, K., Seiden, M., McPherson, D., Piscitello, D., McConachie, A., April, T., Latour, J., & Rasmussen, R. (2020). The DNS in IoT: Opportunities, Risks, and Challenges. *IEEE Internet Computing*, 24(4), 23-32.
39. Hesselman, C., Poortinga-van Wijnen, R., Schaapman, G., & Ruiter, R. (2020, March 10). Increasing the Netherlands' DDoS resilience together. Retrieved on November 3, 2020, from https://www.sidnlabs.nl/en/news-and-blogs/increasing-the-netherlands-ddos-resilience-together
40. Hoorweg, E. & De Koning, R. (2015). Geen digitalisering zonder digitale veiligheid. Capgemini Consulting. Retrieved on February 29, 2020, from https://www.capgemini.com/consulting-nl/wp-content/uploads/sites/33/2017/08/geen_digitalisering_zonder_digitale_veiligheid.pdf
41. HSD (n.d.). Dutch National Cyber Security Centre (NCSC). Retrieved on February 8, 2021, from https://www.thehaguesecuritydelta.com/partners/partner/135-dutch-national-cyber-security-centre-ncsc
42. Hull, B. (2018, April 4). IoT risk and the smart factory: Building cyber resilience. PWC. Retrieved on February 28, 2020, from https://usblogs.pwc.com/industrialinsights/2018/04/04/iot-risk-and-the-smart-factory-building-resilience/
43. Hyslip, T.S. (2020). Cybercrime-as-a-Service Operations. In: Holt, T., & Bossler, A. (eds) *The Palgrave handbook of international Cybercrime and Cyberdeviance*. Palgrave Macmillan, Cham.
44. ISC^{2}NL (2019, May 28). Increasing the resilience of the Netherlands' digital infrastructure together, ISC2NL Cyber Resilience Event Amersfoort, the Netherlands.

Retrieved on February 29, 2020, from https://www.concordia-h2020.eu/wp-content/uploads/2019/11/20190528-isc2nl-ddos-clearing-house-final.pdf

45. Jones, J.A. (2005). An Introduction to Factor Analysis of Information Risk (FAIR). *Risk Management Insight.*
46. Kopp, D., Santanna, J., Wichthuber, M., Hohlfeld, O., Poese, I., & Dietzel, C. (2019). DDoS Hide & Seek: On the effectiveness of a booter services takedown. *Proceedings of the Internet Measurement Conference*, 65-72.
47. Kowtko, M. (2011). Securing our nation and protecting privacy. *2011 IEEE Long Island Systems, Applications and Technology Conference,* Farmingdale, NY, 1-6.
48. KPN (n.d.). Anti DDoS: Geef aanvallers geen kans. Retrieved on January 16, 2021, from https://www.kpn.com/zakelijk/security/network/anti-ddos.htm
49. Kulikova, O., Heil, R., Van den Berg, J., & Pieters, W. (2012). Cyber Crisis Management: A decision-support framework for disclosing security incident information. International Conference on Cyber Security (CyberSecurity), Washington, DC, USA.
50. Kumar, S., & Carley, K.M. (2016). Understanding DDoS cyber-attacks using social media analytics. *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, Tucson, AZ, USA, 231-236.
51. Kurth, M.H., Keenan, J.M., Sasani, M., & Linkov, I. (2018). Defining resilience for the US building industry. *Building Research & Information*, 47(4), 480-492.
52. Labunets, K., Massacci, F., Paci, F., Marczak, S., & Moreira de Oliveira, F. (2017). Model comprehension for security risk assessment: an empirical comparison of tabular vs. graphical representations. *Empirical Software Engineering,* 22, 3017-3056.
53. Lange, T., & Kettani, H. (2019). On Security Threats of Botnets to Cyber Systems. *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*, 176-183, Noida, India.
54. Lean Production (n.d.). Kaizen. Retrieved on January 2, 2021, from https://www.leanproduction.com/kaizen.html
55. Lee, F.Y, & Shieh, S. (2005). Defending against spoofed DDoS attacks with parth fingerprint. *Computers & Security*, 24(7), 571-586.
56. Levy, Y., & Ellis, T.J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science*, 9.

57. Linkov, I., & Trump, B.D. (2019). Resilience Quantification and Assessment. In: *The Science and Practice of Resilience. Risk, Systems and Decisions*, Springer, Cham.
58. Linkov, I., Carluccio, S., Pritchard, O., Bhreasail, A.N., Galaitsi, S., Sarkis, J., & Keisler, J.M. (2020). The case for value chain resilience. *Management Research Review*, 43(12), 1461-1476.
59. Linkov, I., Eisenberg, D., Bates, M., Chang, D., Convertino, M., Allen, J., Flynn, S., & Seager, T. (2013-a). Measurable Resilience for Actionable Policy. *Environmental Science and Technology*, 47, 10108-10110.
60. Linkov, I., Eisenberg, D., Plourde, K., Seager, T., Allen, J., & Kott, A. (2013-b). Resilience metrics for cyber systems. *Environmental System Decisions*, 33, 471-476.
61. Marchese, D., Jin, A., Fox-Lent, C., & Linkov, I. (2020). Resilience for smart water systems. Journal of Water Resources Planning and Management, 146(1), 02519002.
62. McKinsey & Company (2011). Can you hack it? Managing the cybersecurity challenge. McKinsey on Government, 7. Retrieved on February 29, 2020, from https://www.mckinsey.com/~/media/McKinsey/dotcom/client_service/Public%20Sector/PDFS/McK%20on%20Govt/Full%20reports/TG_Autumn_2011_MOG7%20Final.ashx
63. Mell, P., Scarfone, K., & Romanosky, S. (2007). A complete guide to the common vulnerability scoring system version 2.0. In Published by *FIRST-forum of incident response and security* teams, 1, 23.
64. MITRE (n.d.). MITRE ATT&CK. Retrieved on December 23, 2020, from https://attack.mitre.org/
65. Modderkolk, H. (February 6, 2018). In gesprek met Jelle S. (18), die met ddos-aanvallen de Belastingdienst en banken zou hebben platgelegd. *De Volkskrant.* Retrieved at December 12, 2019, from https://www.volkskrant.nl/wetenschap/in-gesprek-met-jelle-s-18-die-met-ddos-aanvallen-de-belastingdienst-en-banken-zou-hebben-platgelegd~b3887d7b/
66. Morali, A., Zamon, E., Etalle, S., & Wieringa, R. (2009). CRAC: Confidentiality Risk Analysis and IT-Architecture Comparison of Business Networks (extended version). Centre for Telematics and Information Technology (CTIT). Enschede.
67. Munnichs, G., Kouw, M., & Kool, L. (2017). A never-ending race. On cyberthreats and strengthening resilience. *Rathenau Instituut*. Retrieved on February 29, 2020,

from https://www.rathenau.nl/sites/default/files/2018-04/report%20A%20never-ending%20race.pdf

68. Musotto, R, & Wall, D.S. (2020). More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime. *Trends in organized Crime*.
69. Nagpal, B., Sharma, P., Chauhan, N., & Panesar, A. (2015). DDoS tools: Classification, analysis and comparison. International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India.
70. NBIP (2018). Impact van DDoS-aanvallen in Nederland. Retrieved at January 30, 2020, from https://www.nbip.nl/nieuws/rapport-impact-van-ddos-aanvallen-in-nederland/
71. NBIP (n.d.-a). NaWas – national Scrubbing Center against DDoS attacks – a not-for-profit organisation. Retrieved on December 28, 2020, from https://www.nbip.nl/en/nawas/
72. NBIP (n.d.-b). The NBIP - Supporting services for Internet providers. Smarter and stronger together for a safe, secure Internet. Retrieved on December 28, 2020, from https://www.nbip.nl/en/
73. NCSC (2019). Cyber Security Assessment Netherlands 2019. Retrieved at December 12, 2019, from https://www.thehaguesecuritydelta.com/media/com_hsd/report/255/document/CSBN2019-EN-def-Web-01-tcm32-405804.pdf
74. NCSC (n.d.-a). Over het NCSC. Retrieved on February 8, 2021, from https://www.ncsc.nl/over-ncsc
75. NCSC (n.d.-b). Nationale anti-DDoS-coalitie. Retrieved on December 29, 2020, from https://www.ncsc.nl/onderwerpen/ddos/het-nederlandse-anti-ddos-initiatief
76. Newman, S. (2019). Under the radar: the danger of stealthy DDoS attacks. *Network Security*, 2, 18-19.
77. Nikolskaya, K., & Minbaleev, A. (2020). Legal Regulation of Incidents Related to DDoS Attacks. *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, Yaroslavl, Russia, 53-55.
78. No More DDoS (n.d.). National Anti-DDoS-coalitite. Retrieved on December 29, 2020, from https://www.nomoreddos.org/

79. Noroozian, A., Ciere, M., Korczynki, M., Tajalizadehkhoob, & Van Eeten, M. (2017). Inferring Security Performance of Providers from Noisy and Heterogenous Abuse Datasets. *WEIS*.
80. Noroozian, A., Korczynski, M., Gañan, C.H., Makita, D., Yoshioka, K., & Van Eeten, M. (2016). Who Gets the Boot? Analyzing Victimization by DDoS-as-a-Service. *International Symposium on Research in Attacks, Intrusions, and Defenses*, 368-389.
81. OASIS (2020-a, November 29). Introduction to STIX. Retrieved on December 19, 2020, from https://oasis-open.github.io/cti-documentation/stix/intro.html
82. OASIS (2020-b, Introduction to TAXII. Retrieved on December 19, 2020, from https://oasis-open.github.io/cti-documentation/taxii/intro.html
83. Osanaiye, O. (2015). Short Paper: IP spoofing detection for preventing DDoS attack in Cloud Computing. *2015 18th International Conference on Intelligence in Next Generation Networks*, Paris, France.
84. Paauwe, C. (February 6, 2018). Oosterhouter (18) opgepakt voor DDoS-aanvallen. *NRC.* Retrieved from https://www.nrc.nl/nieuws/2018/02/06/oosterhouter-18-opgepakt-voor-ddos-aanvallen-a1591135
85. Pieters, W. (2013). Defining "The Weakest Link": Comparative Security in Complex Systems of Systems. Proceedings from *IEEE 5th International Conference on Cloud Computing Technology and Science*, Bristol, UK.
86. PwC (2016, November). Managing emerging risks from the Internet of Things. Retrieved on February 29, 2020, from https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/managing-iot-risks.html
87. Rand, K., Kurth, M., Fleming, C.H., & Linkov, I. (2020). A resilience matrix approach for measuring and mitigating disaster-induced population displacement. *International Journal of Disaster Risk Reduction*, 42, 1-12.
88. Resilience. (n.d.-a). In *Merriam-Webster.com dictionary.* Retrieved from https://www.merriam-webster.com/dictionary/resilience
89. Resilience. (n.d.-b). In *Ofxord Learner's Dictionaries.* Retrieved from https://www.oxfordlearnersdictionaries.com/definition/american_english/resilience
90. Rosenquist, M. (2009). Prioritizing Information Security Risk with Threat Agent Risk Assessment. *IT@Intel White Paper*.

91. Salim, M.M., Rathore, S., & Park, J.H. (2019). Distributed denial of service attacks and its defenses in IoT: a survey. *The Journal of Supercomputing*, 1-44.
92. Sanders, W.H. (2014). Quantitative Security Metrics: Unattainable Holy Grail or a Vital Breakthrough within Our Reach? *IEEE Security & Privacy*, 21(2), 67-69.
93. Santanna, J.J., De Vries, J., Schmidt, R, Tuncer, D., Granville, L., & Pras, A. (2018). Booter list generation: The basis for investigating DDoS-for-hire websites. *International journal of Network Management*, 28(1).
94. Sayagh, M., Kerzazi, N., Adams, B., & Petrillo, F. (2020). Software Configuration Engineering in Practice Interviews, Survey, and Systematic Literature Review. *IEEE Transactions on Software Engineering*, 46(6), 646-673.
95. Sikula, N.R. Mancillas, J.W., Linkov I., & McDonagh, J.A. (2015). Risk management is not enough: a conceptual model for resilience and adaption-based vulnerability assessments. *Environment Systems and Decisions*, 35(2), 219-228.
96. Singh, R., & Sharma, R.P (2019). Present Status of Distributed Denial of service (DDoS) attacks in internet world. *International Journal of Mathematical, Engineering and Management Sciences*, 4(4), 1008-1017.
97. Takaaki, S., & Atsuo, I. (2019). Dark Web Content Analysis and Visualization. *ACM International Workshop on Security and Privacy Analytics*, 53-59.
98. The U.S. National Academy of Sciences (2012). Disaster Resilience: A National Imperative. The National Academies Press: Washington, DC.
99. Thornton-Trump, I. (2019). The politics of cyber. *EDP Audit, Control, and Security Newsletter*, 59(3), 1-17.
100. Van den Berg, J., Van Zoggel, J., Snels, M., Van Leeuwen, M., Boeke, S., Van de Koppen, L., Lubbe, J., Van den Berg, B., & De Bos, T. (2014). On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education.
101. Van Eeten M.J.G., & Bauer, J.M. (2008). Economics of malware. *OECD Science, Technology and Industry Working Papers*.
102. Van Unen, D. (July 31, 2018). DigiD opnieuw doelwit DDoS-aanval. *NRC*. Retrieved on December 12, 2019, from https://www.nrc.nl/nieuws/2018/07/31/digid-opnieuw-doelwit-ddos-aanval-a1611711
103. Verhagen, L. (February 5, 2018). 18-jarige jongen opgepakt in verband met ddos-aanvallen op Belastingdienst. *De Volkskrant*. Retrieved at December 12, 2019,

from https://www.volkskrant.nl/cultuur-media/18-jarige-jongen-opgepakt-in-verband-met-ddos-aanvallen-op-belastingdienst~b3290084/

104. Wang, A., Chang, W., Chen, S, & Mohaison, A. (2018). Delving Into Internet DDoS Attacks by Botnets: Characterization and Analysis. *IEEE/ACM Transactions on Networking*, 26(6), 2843-2855.

105. Watkins, L., Silberberg, K., Morales, J.A., & Robinson, W.H. (2015). using inherent command and control vulnerabilities to halt DDoS attacks. *2015 10th International Conference on Malicious and Unwanted Software (MALWARE)*, Fajardo, 3-10.

106. Webster, J., & Watson, R.T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26(2).

107. Wee, B.V., & Banister, D. (2016). How to write a literature review paper? *Transport Reviews*, 36(2), 278-288.

108. Wienen, H.C.A., Bukhsh, F.A., Vriezekolk, E., & Wieringa, R.J. (2019). Applying generic accimap to a DDoS attack on a Western-European telecom operator. *16th International Conference on Information Systems for Crisis Response and Management, ISCRAM*, Valencia.

109. Wood, M.D., Wells, E.M., Rice, G., & Linkov, I. (2019). Quantifying and mapping resilience within large organisations. *Omega*, 87, 117-126.

110. World Economic Forum, BCG, and & Hewlett Packard Enterprise (2017, January). Advancing Cyber Resilience: Principles and Tools for Boards. Retrieved on February 29, 2020, from http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf

111. You, W., Jiao, L., Li, J., & Zhou, R. (2020). Scheduling DDoS Cloud Scrubbing in ISP Networks via Randomized Online Auctions, *IEEE INFOCOM 2020 – IEEE Conference on Computer Communications*, 1658-1667, Toronto, ON, Canada.

112. Yuan, B., Zhao, H., Lin, C., Zou, D., Yang, L.T., Jin, H., He, L., & Yu, S. (2020). Minimizing Financial Cost of DDoS Attack Defense in Clouds With Fine-Grained Resource Management. *IEEE Transactions on Network Science and Engineering*, 7(4), 2541-2554.

113. Yusof, M., Ali, F., & Darus, M. (2017). Detection and Defense Algorithms of Different Types of DDoS Attacks. International Journal of Engineering and Technology, 9(5), 410-414.

114. Zedner, L. (2003). Too much security? *International Journal of the Sociology of Law*, 31, 155-184.

115. Zheng, X. & Julien, C. (2015). Verification and Validation in Cyber Physical Systems: Research Challenges and a Way Forward. *2015 IEEE/ACM 1st International Workshop on Software Engineering for Smart Cyber-Physical Systems*, Florence, Italy.

116. Zussblat, N.P., Ganin, A.A., Larkin, S., Fiondella, L., & Linkov, I. (2017). Resilience and Fault Tolerance in Electrical Engineering. *Resilience and Risk*, 427-447.

Appendices

Appendix A: Transcripts of the interviews

This version of the thesis does not include the transcripts of the interviews to keep the number of pages reasonable.

Appendix B: Linkov and colleagues' cyber resilience matrix

Table 1: The cyber resilience matrix (Linkov and colleagues, 2013-b)

Plan and prepare for	Absorb	Recover from	Adapt to
Physical			
(1) Implement controls/sensors for critical assets [S22, M18, 20]	(1) Signal the compromise of assets or services [M18, 20]	(1) Investigate and repair malfunctioning controls or sensors [M17]	(1) Review asset and service configuration in response to recent event [M17]
(2) Implement controls/sensors for critical services [M18, 20]	(2) Use redundant assets to continue service [M18, 20]	(2) Assess service/asset damage	(2) Phase out obsolete assets and introduce new assets [M17]
(3) Assessment of network structure and interconnection to system components and to the environment	(3) Dedicate cyber resources to defend against attack [M16]	(3) Assess distance to functional recovery	
(4) Redundancy of critical physical infrastructure		(4) Safely dispose of irreparable assets	
(5) Redundancy of data physically or logically separated from the network [M24]			
Information			
(1) Categorize assets and services based on sensitivity or resilience requirements [S63]	(1) Observe sensors for critical services and assets [M22]	(1) Log events and sensors during event [M17, 22]	(1) Document incident's impact and cause [M17]
(2) Documentation of certifications, qualifications and pedigree of critical hardware and/or software providers	(2) Effectively and efficiently transmit relevant data to responsible stakeholders/ decision makers	(2) Review and compare systems before and after the event [M17]	(2) Document time between problem and discovery/discovery and recovery [S41]
(3) Prepare plans for storage and containment of classified or sensitive information			(3) Anticipate future system states post-recovery
(4) Identify external system dependencies (i.e., Internet providers, electricity, water) [S31]			(4) Document point of entry (attack)
(5) Identify internal system dependencies [S63]			
Cognitive			
(1) Anticipate and plan for system states and events [M18]	(1) Use a decision making protocol or aid to determine when event can be considered "contained"	(1) Review critical points of physical and information failure in order to make informed decisions [M17]	(1) Review management response and decision making processes
(2) Understand performance trade-offs of organizational goals	(2) The ability to evaluate performance impact to determine if mission can continue	(2) Establish decision making protocols or aids to select recovery options	(2) Determine motive of event (attack)
(3) Scenario-based cyber wargaming	(3) Focus effort on identified critical assets and services [M20]		
	(4) Utilize applicable plans for system state when available [M20]		
Social			
(1) Identify and coordinate with external entities that may influence or be influenced by internal cyber attacks (establish point of contact)	(1) Locate and contact identified experts and resilience responsible personnel [S40]	(1) Follow resilience communications plan	(1) Evaluate employees response to event in order to determine preparedness and communications effectiveness [S18, 19]
(2) Educate/train employees about resilience and organization's resilience plan [M17, S29]		(2) Determine liability for the organization	(2) Assign employees to critical areas that were previously overlooked [S22]
(3) Delegate all assets and services to particular employees [S15, 22]			(3) Stay informed about latest threats and state of the art protection methods/share with organization
(4) Prepare/establish resilience communications [S17]			
(5) Establish a cyber-aware culture			

Appendix C: Interview questions and prompts

Table 3: Matrix-based interview questions and prompts.

General area		Prompts
	From your point of view, what factors indicate the system's ability to...	
Domain		
Physical	plan/prepare for a DDoS attack implemented in the physical domain?	controls/sensors for critical assets, controls/sensors for critical services, network structure and interconnection, redundancy of critical physical infrastructure and data
	absorb a DDoS attack implemented in the physical domain?	compromised assets or services, redundant assets for continuing service, cyber resources to defend against attack
	recover from a DDoS attack implemented in the physical domain?	malfunctioning control or sensors, service/asset damage, distance to functional recovery, safety dispose of irreparable assets
	adapt to a DDoS attack implemented in the physical domain?	review of asset and service configuration in response to attack, phased out obsolete assets ad introduction of new assets
Information	plan/prepare for a DDoS attack implemented in the information domain?	categories of assets and services based on sensitivity or resilience requirements; documentation of certifications, qualifications and pedigree of critical hard- and software; plans for storage and contrinament of classified or sensitive information; external system dependencies, internal system dependencies
	absorb a DDoS attack implemented in the information domain?	observations of sensors for critical services and assets, transmitting of relevant data to responsible stakeholders/decision-makers
	recover from a DDoS attack implemented in the information domain?	log events and sensors during event, reviews and comparisons of systems before and after the event
	adapt to a DDoS attack implemented in the information domain?	documentation of impact and cause, documention of time between attack and discovery and between recovery, anticipation on future system states, documentation of attack's entry
Cognitive	plan/prepare for a DDoS attack implemented in the cognitive domain?	plan for attack, understanding on performance trade-offs, scenario-based cyber wargaming
	absorb a DDoS attack implemented in the cognitive domain?	decision-making protocol or determination when attack can be considered contained, ability to evaluate performance, effort on identificatied critical assets and services, utilization of applicable plan for system state when available
	recover from a DDoS attack implemented in the cognitive domain?	review of critical points of physical and informational failure, decision-making protocols to select recovery options
	adapt to a DDoS attack implemented in the cognitive domain?	review of management response and decision-making processes, determination of motive of attack
Social	plan/prepare for a DDoS attack implemented in the social domain?	identification and coordination with external entities (point of contacts), education of employees about resilience and resilience plan, delegation of all assets and services to particular employees, preparation resilience communications, cyber-aware culture
	absorb a DDoS attack implemented in the social domain?	location and contact with identified experts and resilience responsible personnel
	recover from a DDoS attack implemented in the social domain?	following of resilience communications plan, liability for the organization
	adapt to a DDoS attack implemented in the social domain?	evaluation employees response to event (preparedness and communication effectiveness), assignment of employees to critical areas that were previously overlooked, informedness on latest threats and protection methods