Fighting Child Sexual Abuse Material better together

A stakeholder central review on the government policies against CSAM

Marie Sam Rutten

TU Delft

Fighting Child Sexual Abuse Material better together, a stakeholder central review of the government policies

by

Marie Sam Rutten

to obtain the degree of Master of Science in Engineering and Policy Analysis

at the Delft University of Technology,

to be defended publicly on 17th of February

Student number:	4349245	
Project duration:	August 31, 2020 – January 29, 2021	
Thesis committee:	Prof. dr. M. J. G. van Eeten,	TU Delft, Chair
	dr. R. S. van Wegberg,	TU Delft, First supervisor
	dr. -Ing. T. Fiebig,	TU Delft, Second supervisor
	ir. Q. B. Lone,	TU Delft, Advisor

On behalf of the Ministry of Justice and Security

Preface

Dear reader,

Thank you for taking the time to read the preface of my thesis. This report serves as my thesis for the Engineering and Policy Analysis master at Delft University of Technology. However, more so I hope this report will function as a starting point to a more thoroughly cleansing the Internet of CSAM, and policies addressing illegal content and cybercrime by means of a true private-public collaboration.

The past year I got the opportunity to support the program against CSAM and the Cybercrime team in their social responsibility to protect the Dutch citizens of these crimes. Those teams provided me with a lot of knowledge about the working of the Dutch government, political processes and the collaboration with internal and external parties. Actively participating in the policymaking process concerning CSAM and cybercrime truly opened my eyes. Policymaking on topics affiliated with the Internet sector is relatively new, dynamic and surprising and requires close collaboration with all involved stakeholders.

Furthermore, I'm very grateful to be part of a team of highly motivated people dedicated to create a safe Netherlands, who still took the time to have some fun and even managed to answer all my questions. With special thanks to Pepijn Sleyfer, who did not only guide me through my whole Internship but was also an essential part of my thesis committee.

Moreover, I would like to thank Rolf van Wegberg for always making time to answer my questions, think along, giving relevant advice or simply highlighting that it was my thesis, and I should not ponder to much about everyone's preferences. Also, I thank Michel van Eeten for his very critical view on my work and helping me with getting this internship without knowing me very well. Furthermore, I thank Qasim Lone for his support, enthusiasm about my thesis topic and all his help. Qasim's passion is contagious and it motivated me again and again to work on this thesis. At last, from my committee, I would also like to thank Tobias Fiebig for providing me with great insights into the working of the Internet.

My time in Delft has been wonderful and definitely wouldn't be the same without my family and friends. They always supported me unconditionally and helped again and again when I created too much work for myself. Special thanks go to Isabelle: without you my thesis would not have been of this quality. Last but not least, I want to thank Ivar for literally always helping me and making me smile!

Marie Sam Rutten

Summary

Background

This study aims to make recommendations about how the Internet can be more thoroughly cleaned of Child Sexual Abuse Material (CSAM), focusing on the Dutch government policies. In the past years, several organizations, including the European Commission, called out the Netherlands for the role Dutch companies have in the hosting of CSAM. According to INHOPE, the CSAM hotline umbrella organization, the Netherlands is responsible for 20% of the hosted CSAM worldwide and 79% within the EU.

In 2017 the just appointed Minister of Justice and Security (Ministry of J&V), Ferdinand Grapperhaus, and the Secretary of State of the Ministry of Economic Affairs and Climate policies (Ministry of EZK), Mona Keijzer, re-prioritized the fight against CSAM. One of the four lines is: "Cleaning the Internet of CSAM: Public-private collaboration (PPC) and the introduction of a regulatory approach", which is expected to have the most considerable and most immediate effect on the amount of CSAM on the Internet. The policy "Cleaning the Internet of CSAM: Public-private collaboration (PPC) and the introduction of a regulatory approach" develops around four government policies:

1. Transparency: TU Delft monitor
2. Self-regulation: Code-of-Conduct CSAM addendum
3. Framework for action: HashCheckService (HCS)
4. Regulatory approach: administrative law to issue fines to non-compliant hosting providers

The above named four government policies are established, implemented, and executed in the spheres of the PPC. The working group of the PPC consists of stakeholders involved in the cleaning of the Dutch Internet of CSAM and includes, among others, industry representatives of the hosting sector, the Dutch Online Child Abuse Expert Office and hotline (EOKM), the national police teams engaged in Combating Child Sexual Abuse and the Exploitation of Children in the Context and Tourism (TBKK) and officials of the Dutch government (Grapperhaus, 2018b). Furthermore, the government policies' success is also influenced by stakeholders who do not take place in the PPC, as foreign hotlines and the European Commission (EC).

Problem definition

Two study area's are interesting to consider regarding CSAM government policies. Firstly, regulating abuse and specifically illegal content online. Secondly, studies concerning the working of the Notice-and-Takedown (NTD) mechanism and affiliated instruments. Based on the literature, three knowledge gaps are identified, namely, (1) there is little research that identifies real-world execution and processes of the CSAM NTD mechanism and other instruments like the HCS, (2) the influence of stakeholders' positions and their participation in the policymaking process on CSAM government policies have not been studied, and (3) in research there is lack of an overview of the effects of the current government policies and possible improvements to them. These research gaps make it difficult for the Dutch government to oversee the possible pitfalls and areas of improvement of the policies.

Therefore, this study focuses on filling these three research gaps and aims to make recommendations on how the Dutch government policies can be improved. The main research question is:

How can the Dutch government policies clean the Internet from Child Sexual Abuse Material (CSAM) be improved?

Methodology

For this study, a mixed-methods approach is chosen. A mixed-methods approach combines a qualitative and a quantitative method. The qualitative analysis is used to reveal relevant stakeholders, their positions, how they participate in the policymaking process, how they evaluate the government policies, and what they believe are the most significant improvements to the system. The quantitative analysis aims to complement the already existing data and provide more quantitative insights into the government policies.

The quantitative results map information flows and processing times of the Dutch CSAM NTD mechanism. The results are obtained through data analyses of the data provided by INHOPE, EOKM, the Canadian hotline, and IWF. Semi-structured interviews are used to gather qualitative data. During the study, 21 interviews with 19 different organizations are conducted. The different organizations are: EOKM, hosting providers, foreign hotlines, industry representatives, the RIPE NCC community, INHOPE, the Ministry of J&V, the Ministry of EZK, DG HOME of the EC, and TBKK.

The results of the semi-structured interviews aim to gather data in three area's. Firstly, the interview data are used to identify organizations' internal processes in the NTD and affiliated instruments. Secondly, the stakeholders' position regarding the government policies and how they participate in the policymaking process is asked. Finally, the interview data is used to evaluate the government policies and provide an overview of relevant improvements.

Results

Combining the qualitative and quantitative research has led to several key insights.

Firstly, hotlines have an indispensable role in the government policies. Therefore, a combination of a higher automation degree and enough capacity is necessary to ensure their adequate functioning. The majority of the hotlines note to struggle with capacity limitations, including EOKM. Capacity limitations result in back-logs, impossibility to monitor all reports, and limited guidance to the sector. Automatic systems and technologies like PhotoDNA help to lighten the workload. However, hotlines have a competitive relationship, and it is unlikely that they will share all technologies. Moreover, to assure a thorough process, not all acts can be replaced by automatic systems.

Secondly, the sector's low organizational degree is a hurdle/difficulty/obstacle for acts of self-regulation, co-regulation, and regulation efforts. A low organizational degree makes it challenging to create widely supported policies, spread established policies, monitor policies' compliance, and issue sanctions when policies are violated. Also, a significant part of the sector feels not represented by the industry organizations and therefore believe to have little influence on the government policies. A better organization will enhance the sharing of best practices. Sharing best practices can help the industry optimize processes and determine what kind of instruments and policies are effective and feasible. Better organization will also increase the influence of the sector on the government policies. Furthermore, with already effective established self-regulation, the government can follow those lines and uncomfortable laws and policies would be prevented from being established.

Thirdly, the current classification used in the government policies seems to categorize all the companies into the same group of "hosting providers". This classification is legally inaccurate and also nonspecific. The classification does not reflect the high diversity of the Internet intermediates addressed in the government policies. The kind of services Internet intermediates offer determine their different levels of access to the networks of their clients. Consequently, their services determine the possibilities to respond to CSAM takedown requests. Furthermore, not all norms the hosting providers need to comply with are evident to the sector. Setting norms and implementing policies can significantly influence the economic welfare of the sector, safety on the Internet, privacy, and Internet freedom. Before setting a norm or implementing a policy, it should be considered which instruments are needed to reach such norms and its consequences for the different hosting providers and Internet users.

Fourthly, With the NTD mechanism, much CSAM content remains unfound. A broader adaptation of the HCS will help to reveal the hosted CSAM. However, this study showed that unknown companies are not likely to implement the HCS if they are not aware that they host any CSAM. During the interviews, proactive searching with an automatic crawler for known CSAM is a solution to reveal more companies hosting CSAM.

Next, in general, TBKK struggles with effectively investigating offenders affiliated with online CSAM that are not directly involved in sexual child abuse. Due to both of limited financial and staff capacity. During the interviews, it was addressed that the law enforcement needs to get more adequate. However, academic literature and reports give little guidance on how law enforcement can be strengthened.

Furthermore, for most proposed improvements, structural financial resources are necessary. The interviewed stakeholders in this study have conflicting opinions about who should pay what and why. A structural financial system needs to be established in order to assure adequate policies in the future.

Finally, this research shows that hosting providers handle illegal content and abuse with the same procedures and use the same systems when handling the CSAM. Consequently, the NTD procedures and the whole CSAM government policies should be more connected with policies against abuse in general.

Recommendations

Based on the conclusion and discussion, seven recommendation to improve the government policies on cleaning the Internet of CSAM are made:

1. Establish an industry liaison
2. Enable in the Netherlands or the EU proactive searching of CSAM
3. Support the sector in enlarging the self-regulation
4. Communication to the sector
5. Strengthen the processes of EOKM
6. Commission a study on how law enforcement can be more fitting for online crimes
7. Develop a proactive Europe strategy and actively try to influence the initiatives of the European Commission

Keywords: Notice-and-takedown, Child Sexual Abuse Material (CSAM), Regulation, Participation, Rounds model, Stakeholder perspective

Contents

Abbreviation

Ministry of J&V = Dutch Ministry of Justice and Security
Ministry of EZK = Dutch Ministry of Economic Affairs and Climate Policies
NTD = Notice-and-Takedown
CSAM = Child Sexual Abuse Material
CSA = Child Sexual Abuse
EC = European Commission
EU = European Union
EOKM = Online Child Abuse Expert Office
TBKK= Police Teams engaged in Combating Child Sexual Abuse and the Exploitation of Children in the Context and Tourism
IWF = International Watch Foundation
NCMEC = National Centrum for Missing and Exploited children
CSE = Child Sexual Exploitation
ASN = Autonomous System Number
DSA = Digital Services Act

1

Introduction

Online Sexual Child Abuse Material (CSAM) is degrading and one of the most destroying forms of criminality – Minister of Justice and Security F. Grapperhaus (2019b)

The spread of Child Sexual Abuse Material is traumatizing and very harmful for children. The returning exposure of old material is re-victimizing. Furthermore, online CSAM can normalize child abuse for downloaders and for possible future abusers. Available online CSAM maintains the profitability of production and sharing of CSAM, endangering more children (Broadhurst, 2019; Demeyer et al., 2012).

With the rise of the Internet and associated technologies, the spread and downloading of Child Sexual Abuse Material (CSAM) are thriving. Nowadays, offenders, downloaders, and distributors use the Internet as the primary communication channel for the spread and search for CSAM (Steel et al., 2020). There has been a significant increase of material found online in the past years, also in the Netherlands (INHOPE, 2018). From 2013 to 2019, the Dutch Online Child Abuse Expert Office and hotline (EOKM) has experienced an increase of 30% to 40% of reported CSAM each year (EOKM, 2020, 2018, 2016). According to the International Watch Foundation (IWF), the Netherlands hosted 71% of the worldwide known CSAM in 2019 against 47% in 2018 (Internation Watch Foundation, 2020). Dutch Internet infrastructure is used to host CSAM online. Dutch IP-addresses and servers on Dutch soil are operated by hosting providers or other Internet intermediates (Alaerds et al., 2017; Noroozian et al., 2019). Those Internet intermediates provide online access to a large share of the worldwide CSAM (DHPA, 2019; IXPDB, 2020). Hence, in 2020 the European Commission has called out the Netherlands as the leading facilitator of CSAM on the internet (European Commission, 2020a)

In 2017 the just appointed Minister of Justice and Security (Ministry of J&V), Ferdinand Grapperhaus, and the Secretary of State of the Ministry of Economic Affairs and Climate policies (Ministry of EZK), Mona Keijzer, re-prioritized the fight against CSAM. The Dutch government developed the renewed program against CSAM, consisting of three policy lines:

1. Intensifying prevention: focused on victims, offenders of abuse, and downloaders;

2. Cleaning the Internet of CSAM: Public-Private Collaboration (PPC) and the introduction of a regulatory approach;

3. Strengthen the investigative system (**?**)

The second policy line, "Cleaning the Internet of CSAM: Public-private collaboration (PPC) and the introduction of a regulatory approach", is expected to have the most considerable and most immediate effect on the amount of CSAM on the Internet. The second policy lines develop around four government policies: (1) Transparency, (2) Self-regulation, (3) Framework for action, and (4) Regulatory approach. Those four government policies to clean the Internet of CSAM (hereafter referred to as government policies) are established, implemented, and executed in the spheres of the PPC. The PPC consists of stakeholders involved in the cleaning of the Dutch Internet of CSAM and includes, among others, industry representatives of the hosting sector, EOKM, the national Police Teams engaged in Combating Child Sexual Abuse and the Exploitation of Children in the Context and Tourism (TBKK) and the Dutch government (Grapperhaus, 2018b).

The Notice-and-Takedown (NTD) mechanism is central to the government policies "Transparency" and "Self-regulation" (Grapperhaus, 2018b). The NTD mechanism is a self-regulatory instrument aimed at noticing and taking down abuse of the Internet by the Internet sector (Anti Abuse Netwerk (AAN), 2020). The integral NTD mechanism of CSAM consists of detecting, aggregating, verifying, reporting, and removing CSAM of the Internet (Akdeniz, 2008). Under the policy "self-regulation" PPC, the hosting sector committed to taking down reported CSAM within 24 hours (Grapperhaus, 2018b; Noticeandtakedown.nl, 2018a). For the policy "Transparency", the TU Delft has developed a monitor that maps which hosting provider hosts how much CSAM and how fast they take it down on behalf of the Dutch government. The Dutch government published the TU Delft monitor report in October 2020 containing the performance of the hosting providers. In June 2020, the Dutch government warned hosting providers for the upcoming monitor with a "warning letter" (Grapperhaus, 2020b). Due to the involvement of the government, the regulation of the NTD mechanism has moved from self-regulation to co-regulation.

With the policy "framework of action," the PPC attempts to provide the hosting sector with instruments to clean and keep cleaning their services from CSAM. The most prominent instrument is the HashCheckService (HCS), a hash (digital fingerprint of content) database that Internet companies can use to check if they host CSAM on their servers (Grapperhaus, 2018b). For the policy "Regulatory approach" the Dutch government will introduce an administrative law. Under this law, a newly established regulator can issue fines if hosting providers do not take down reported content within 24 hours (Steur et al., 2019).

Although the government actions is a start to clean the Internet of CSAM, there are many unknowns regarding the working and effectiveness of the new polices (Wang, 2018; European Parliament, 2020; Kokolaki et al., 2020). It is expected that the current policies will not be sufficient to thoroughly clean the Internet of CSAM, improvements to the government policies. Not much research is done in this regard. It is unknown which factors influence the adequacy of the government policies (Holt et al., 2020). The large number and diversity of the involved stakeholders make it difficult to oversee the policy making processes (Bauer and van Eeten, 2009; Açar, 2020). Moreover, the public-private character of the government policies makes stakeholders and their expertise vital for the government policies. Including stakeholders in any evaluation of the government policies is therefore essential.

1.1 Research objective

The first research objective is to identify the most important pitfalls within current government policies. The research outcomes will mainly be based on the stakeholder's perspectives due to the high dependency on stakeholders in the process of policy making, implementation, and execution. Furthermore, in an attempt to weigh the perspectives of stakeholders, a quantitative analysis is performed on the information flows and processing times of the NTD mechanism and the HCS. Academic studies on the regulation of illegal content will function as a starting point for this investigation.

The second objective of this research is to translate the identified pitfalls into useful recommendations for the Dutch Government to clean the Internet of CSAM more thoroughly and also faster.

1.2 Research scope

The Internet has blurred jurisdictional borders, and the CSAM NTD mechanism consists of a worldwide network with a multitude of organizations. However, The government policies to clean the Dutch Internet infrastructure have a national focus. The predominant focus of this research lies, therefore, on Dutch organizations involved in government policies. However, some international organizations such as the EC and foreign hotlines have a significant influence on the government policies and are therefore included in the study.

1.3 Research questions and approach

Based on the a background study in Chapters 2, 3, and 4 the main research question is formulated:

How can the Dutch government policies to clean the Internet from Child Sexual Abuse Material (CSAM) be improved?

A mixed-methods approach is used to answer the main research question. In line with the research approach, the following research sub-questions are identified to answer the main research question:

1. How does the Dutch NTD mechanism and the HashCheckService look like in terms of processes, information flows, and processing times per organization?

2. Who are the relevant stakeholders, and what is their position regarding the government policies to clean the Internet of CSAM?

3. How do the relevant stakeholders participate in the policymaking process?

4. How do the stakeholders evaluate the current government policies?

5. What are the most relevant policy improvements suggested by the stakeholders?

Chapter 3 outlines the current status of the fight against CSAM. Chapter 4 is dedicated to the NTD mechanism. In chapter 5, the methodology is described. In chapter 6, the quantitative analysis and the process descriptions based on the interviews are stated. In chapter 7, the interviews' results concerning stakeholders' position, the participation of stakeholders in the policymaking process, the evaluation of the government policies, the combined quantitative and qualitative results, and the suggested improvements are presented. The discussion, conclusion, and recommendations for the Ministry of Justice and Security are discussed in chapter 8.

1.4 Academic contribution

– Knowledge gap This research contributes in three ways to the academic field. Firstly, it will attempt to identify real-world execution and processes of the CSAM NTD mechanism and other instruments like the HCS. Secondly, it will map the influence of stakeholders' positions and their participation in the policymaking process on CSAM government policies. Thirdly, this research tries to provide an overview of the effects of the current government policies and possible improvements to them. Altogether, this research presents a unique combination of a quantitative and a qualitative analysis of the current government policies to clean the Internet of CSAM.

1.5 Linkage with EPA study program

This research perfectly fits in the EPA master's program since it contributes to a solution for a complex socio-technical Grand Challenges the world is currently facing. The regulation of CSAM reflects the interaction between technology and society. Policies are established, implemented, and executed in a multi-stakeholder environment. The EPA program teaches several instruments to evaluate complex policy challenges. In line with the program, this research combines a quantitative data analysis with a qualitative interview method. Hence, both the systematic and the political pitfalls and challenges are addressed.

2

Fighting illegal content

2.1 Criminal activities and abuse on the Internet

The Internet is a meeting, market, and sharing place for people. You can work with your colleagues; you can meet new people, you can do your groceries, you can manage your financials, and so on. The Internet also makes it easier to conduct criminal or undesirable activities such as; financial fraud, infringement, and illegal drug trade (Holt et al., 2020; Europol, 2019). Furthermore, sharing opinions and content which are not common, not socially accepted, or even illegal became more manageable with the invention of the Internet. Everyone can connect anonymously with like-minded people worldwide without being censored (Abdullah, 2019). Content is shared in just seconds, and the billion domains and fora serve as safe havens for undesirable activities. There are two categories of "undesirable" phenomena on the Internet; 1. cybercrime, 2. crimes conducted on the Internet (Charalambous et al., 2016). The difference can be assessed by looking at how it can be determined if it is illegal according to national law (van Eeten et al., 2016; van Hoboken et al., 2020; European Parliament, 2020).

Cybercrime

Cybercrime includes criminal activities that can only be conducted on the Internet. These are criminal phenomena such as Distributed-Denial-of-Service (DDoS) attacks, Man-in-the-Middle (MitM) attacks, and ransomware attacks. Cybercrimes easily are recognized by assessing the technical specifications of the Internet activity, e.g., is the data intercepted or blocked (Jhaveri et al., 2017; van Eeten et al., 2016).

Crimes conducted on the Internet

Crimes conducted on the Internet are everyday crimes that always existed but are now moved to the Internet. Some of these phenomena are thriving, profiting from the Internet's speed, anonymity, and reach (Cooper, 1998; Holt et al., 2020). There are roughly two types of crimes: 1. Illegal activities, 2. Illegal/harmful content. Illegal activities are the performance of an act that is illegal but not the content (Zulkarnine et al., 2016; European Parlaiment, 2020). For example, sharing a picture of a weapon is not illegal but selling a weapon is . Illegal or harmful content is determined by assessing the content which appears on the Internet. In the Netherlands, it is, for example, illegal to share a video in which people are stimulated to perform terrorist attacks because the content violates the national law (European Parliament, 2020; Ognyanova, 2014).

Illegal contet

There are multiple degrees of undesirable or harmful content; 1. Illegal content, 2. Unlawful content, and 3. Harmful content. The most severe category is illegal content. The European Parliament (2020) defines illegal content as: "Any information that is not compliant with EU law or the law of a Member state. Including terrorist content, child sexual abuse material, illegal hate speech, commercial scams, and frauds or breaches of intellectual property rights", and are applied to cyberspace. In general, states follow the line of what is illegal offline is illegal online. Unlawful content is not always illegal but can be illegal depending on the context and situation. An example is a nude picture from someone on the Internet which is shared without their permission (van Hoboken et al., 2020). A nude is not illegal, but if the person did not give permission to share the picture, it is. Lastly, the category of "harmful content". Harmful content not (directly) illegal but can still be undesirable due to its possible impact, as the spread of fake news. Sharing something which is not true is not illegal, but it can have significant consequences(Yar, 2018; European Parlaiment, 2020). For example, with the COVID-19 crisis, fake news was spread that drinking chlorine would protect you from the virus. Although it is not true, it can be very harmful to people's health. It can even cause death. There is a difference in regulating illegal, unlawful, and harmful content. For the latter two, it is dependents on the context, situation, and effect if something is indeed illegal or harmful or not. Consequently, it is almost impossible to filter preventive content as it can violate human rights such as freedom of expression and lead the over-censuring (Council of Europe, 2016). Although illegal content faces some similar challenges, it is the least ambiguous category and most (directly) sever category (Keen et al., 2020)

Sharing, downloading, or searching illegal content also exists in the physical world. However, the number, the impunity, and the impact of the incidents are many times larger on the Internet. Partly due to the characteristics of the Internet. In the physical society, the spread of harmful or non-socially accepted "content" is limited by law enforcement and social control (Von Behr et al., 2013; Bae, 2017; Wijk et al., 2019). If you are standing on a square waving the flag of Nazi Germany, in no time will people either have called you out or called the police. You will often experience consequences for your needs. At least you know there is a possibility you will face the repercussion of law enforcement. Law enforcement on the Internet is more complicated than in the physical world. States are pondering how to regulate content on the Internet analogous to physical society while respecting their citizens' human or ground rights of their citizens (Kaur and Tao, 2014; Yar, 2018; Keen et al., 2020).

2.2 Challenges of regulating illegal content

Governments are struggling with regulating illegal content because of the technical possibilities, conflicting human rights, the Internet (sector) structure, and blurred jurisdictional laws and borders. Further, assessing the illegality of the content is challenging (Yar, 2018; Steel, 2009; Keen et al., 2020). Understanding and creating effective policies are only possible with a deep understanding of those topics.

Firstly, technologies aimed at anonymity and secrecy allow offenders to hide their illegal actions and possibly reduce psychological distress. Offenders are less reluctant to offend as there is a smaller chance of being caught. Well-known technologies used by offenders are VPNs, peer-to-peer networks, the Onion Router (ToR), encryption and wiping software (Steel et al., 2020; Holt and Bossler, 2020). These technologies have two main implications for the regulation: 1. more and more illegal content is shared online, 2. it is hard for Law Enforcement Agencies (LEAs) to reveal the identity of offenders, find and prosecute them (Zulkarnine et al., 2016).

Secondly, the illegality of content can only be assessed by looking at the material. The material assessment is time-consuming and still often needs to be checked by a human pair of eyes or even a judge. More often, the assessment process for pictures and sometimes video's can be executed automatically, through the use of AI programs or with the use of hash-codes (comparable to fingerprints of photos) or pixel recognition (Ramešová, 2020; Wang, 2018). Nevertheless, new or severely altered pictures and photos need to be checked by humans (Ammar, 2019). Additionally, some forms of illegal content are more complex to assess as the context needs to be considered. Human intervention is costly, and that poses a challenge for regulation illegal content (Ramešová, 2020).

Thirdly, governments continuously try to balance human rights as freedom of speech, privacy, and the rule of law (Ramešová, 2020; Ammar, 2019; Jørgensen and Zuleta, 2020). For example, protecting citizens under the rule of law is only possible when the national LEA can find and prosecute offenders. However, with the current protection by anonymity technologies, offenders can (continuously) post illegal content on the Internet with impunity(Kaur and Tao, 2014). The police should be able to "break" technologies such as encryption to protect citizens and perform their tasks under the rule of law. However, giving the police a way around encryption means making it weaker and risk the citizens' privacy. This example illustrates the tension between different human rights and the rule of law (Abdullah, 2019).

Further, the structure of the Internet (sector) causes a complex environment to regulate for governments. The Internet's current registration systems and structure make it difficult for LEAs and governments to reveal which company or person is responsible for the illegal content (Yar, 2018). Also, it is almost impossible to prove that a company willingly knowingly facilitated illegal content. The European e-commerce directive A.14 stipulates that hosting providers are not responsible for the material they host if they are not aware of the material. Accordingly, they are also not obligated to monitor their servers actively (Ramešová, 2020). The Internet (structure) makes it easy to move around content between servers, domains, and providers not to be taken down or investigated. Consequently, investigating any crimes on the Internet is difficult and time-consuming (Hutchings et al., 2016; **?**).

Lastly, blurred jurisdictional laws and borders are challenges for law enforcement and regulation of illegal content online. Due to the Internet's characteristics, if you find something, you have no idea where in the world it is hosted. The sovereignty of states limits national LEA's to regulate illegal content not hosted on their territory. Consequently, it is essential to work closely with other national LEAs, which can be a significant challenge. Moreover, conflicting national laws leading some investigations to a dead end with no results. Although there are some international guidelines, national guidelines are not always aligned. Furthermore, rules in the cyber domain are often not yet anchored in the national law(Abdullah, 2019).

These challenges are not possible to solve solely by (national) LEA's. Integral policies in which private and public organizations actively contribute to counter illegal online content are vital.

2.3 Countering illegal online content through public-private collaborations

Governments all around the world are debating about and trying to regulate (illegal) content online. Since the mid-1990s, the European Union is discussing how to regulate and fight illegal content online (Jørgensen and Zuleta, 2020; European Parliament, 2020; European Commission, 2016). Also, in the Democratic Peoples Republic China (China), the Russian Federation (Russia), and the United States of America (US), this topic of regulating illegal content is a reoccurring topic in policy-makers' agendas and strategies. Although all states have roughly the same goal, "limiting the negative effects of harmful content online", the way they do it and what they consider as harmful is diverse (Chung, 2008; Pollicino and Soldatov, 2018). Many countries outside the European Union have a broader definition of "illegal and harmful content'. Nevertheless, no matter what definition is given, the fight against illegal content is always done through public-private collaboration.

Gate-keeping and self-censorship in China

Chinese Internet content regulation is one of the most rigorous in the world (Chung, 2008). The regulation is roughly based on two pillars: 1. Gate-keeping, 2. Self-censorship (Endeshaw, 2004). Gatekeeping is mostly translated into the great firewall of China. The firewall allows the government to filter and block undesirable or harmful domains (Griffiths, 2019). This way, the government decides which websites the Chinese population can access. It makes it easier to regulate which content enters the Chinese online society. Domains that do not comply with the law can get easily blocked (Lacharite, 2002). The strict gatekeeping at the board of the Chinese Internet results in that most of the domains and applications used solely designed for China. It creates a kind of parallel Internet space. Furthermore, filtering of content is done mostly automatically or in large quantities. That way, often, more than only the illegal or harmful content is blocked (McIntyre, 2013).

The firewall also plays an essential role in stimulating self-censorship. People living within China almost always need to register their identity with a passport or social security numbers before posting content online. It is easier for LEAs to prosecute people (King et al., 2014). In practice, relatively more people are being prosecuted for illegal content-related crimes in China than in the west. Furthermore, because of the limited anonymity on the Internet, people are also more often held responsible for the content they post by society, e.g. by their employers (Pan and Zhang, 2019; MacKinnon, 2009). Due to the more aggressive law enforcement and societal consequences, people within China censor themselves more often (Endeshaw, 2004).

Civilian cyber patrol, monitoring and registering in Russia

The Russian approach is closer to content regulation in the "general" cyberspace used worldwide. Russia does not have a ground on which they rigors block and filter domains and applications. The Russian approach is based on three building blocks: (1) Registering, (2) Monitoring, and (3) Patrolling (Deibert and Rohozinski, 2018).

All ISPs and hosting providers must register at a local authority. Utilizing rigorous registering, the Russian government maps the networks of the Russian Internet infrastructure (Deibert and Rohozinski, 2018). Besides, bloggers with more than 3000 followers need to register. Consequently, if an Influential blogger shares harmful content, LEA's can quickly identify and prosecute this person (Pollicino and Soldatov, 2018). Furthermore, the Russian government monitors the Internet on a vast scale. Similar to the European Union, all information about Russian people needs to be saved on Russian soil. That way, it is easier for the Russian government to enforce laws and prosecute wrongdoers for sharing illegal or harmful full content. Also, in Russia, relatively more people are prosecuted for illegal content crimes than in the west (Ognyanova, 2014). Finally, the Russian government uses non-governmental agencies and civilians to patrol the Internet. Those agencies work closely with Russian law enforcement agencies. Civilian patrollers gather information, notify law enforcement, and can (temporary) takedown domains. This way, the Russian police can scan much larger areas of the Internet and take down illegal content faster (Daucé et al., 2019).

End of Safe-haven regime in Western countries

The primary policy strategy in the west (European Union (AU), United States of America (US), Canada, Australia, New Zealand, and so on) is self-regulation. With the European e-commerce directive adopted in 2000, the European Union moved away from so-called legal intermediate liability. Also, the US adopted in 2000 a law in which intermediate liability was limited (Anchayil and Mattamana, 2010; Moore and Clayton, 2009a). That means that Internet intermediates offering hosting, mere conduit, or caching services cannot be held responsible for the content stored on their servers or passing through their network if they do not know the content. Those internet intermediates are also not obliged to monitor it. Intermediates have an incentive to know as little as possible. It also means that governments have little possibility to enforce regulating illegal content (DLA Piper, 2014; Holt and Bossler, 2020). Therefore, the foundation of illegal content regulation is self-regulation. The most crucial element of this self-regulation is the Notice-and-Takedown (NTD) mechanism (Council of Europe, 2016). The NTD mechanism is a self-regulation instrument for the handling of abuse online. There exist many different NTD mechanisms for all forms of illegal content and cybercrimes. Within the NTD mechanism, content is notified to the internet intermediates. Consequently, they know what content is on their servers, and they need to take action (Moore and Clayton, 2009a).

In the past years, the strategy of western countries is slowly shifting. While keeping the NTD mechanism as a central instrument, other policy lines are considered, adopted, and implemented (Yar, 2018). The European Commission (EC) already dived into the fight against terrorist content online. In line with the directive "combating terrorism" of 2017, the EC did a proposal in which hosting providers are responsible for taking down material within one hour (European Commission, 2020b). Further, Germany also introduced a law called Netz, which obligates providers to take down reported illegal content within 24 hours (van Hoboken et al., 2020; Ammar, 2019). France introduced a similar law for hate speech, but this law was declared unconstitutional (Mouron, 2020). The European Union has also decided that intermediate liability needs to be reformed concerning the e-commerce directive of 2000. In the upcoming Digital Services Act, this reform will be anchored in line with the terrorist content regulation and laws of Germany (European Parlaiment, 2020).

While on the one hand regulating illegal content is taking more shape, on the other hand, the concern about privacy and freedom of speech is ever strong (European Commission, 2019). The willingness to protect fundamental rights motivates western states to keep some control into their own hands and create or stimulate the creation of independent public organizations that check content on their illegality (Ramešová, 2020; Ammar, 2019; Angelopoulos and Smet, 2016).

3

A special form of online illegal content: CSAM on the Internet

Child Sexual Abuse Material is a form of illegal content online. The production, distribution, and downloading of CSAM are terrible and dehumanizing forms of criminality (Grapperhaus, 2018a). Since the founding of the Internet, the increasing distribution of Child Sexual Abuse Material (CSAM) is an ever-growing concern for national and supernational governments. A similar increase is observed for other forms of illegal content(Holt and Bossler, 2020). The returning exposure of this material is re-victimizing children over-and-over again, also later in their lives. It could even normalize child abuse for downloaders and (possible) future abusers. Lastly, it maintains the profitability of production and sharing of CSAM, endangering more children (Broadhurst, 2019; Demeyer et al., 2012; Wijk et al., 2019). In this chapter, it is described how CSAM is hosted and exchanged on the Internet. Furthermore, the regulations with particular attention to the government policies regarding cleaning the Internet of CSAM are discussed.

CSAM is often spread through the use of hyperlinks to domains on the open web. Offenders do not just search in google for material but find it through intermediate platforms. An example of an intermediate website is a forum. Intermediate websites are on the open or dark web (Kokolaki et al., 2020; Westlake and Bouchard, 2016). Also, offenders share links and content in peer-to-peer networks (Bissias et al., 2016). When a hyperlink is shared, offenders only have to click on it and be redirected to a web page with CSAM. Most of the hyperlinks redirect to pages on the open web (Westlake and Bouchard, 2016). offenders prefer the open web due to the high speed with which content can be opened and downloaded. Offenders exchange on the Internet which domains are most suitable to post CSAM. One of the characteristics of suitability is a long time before CSAM is taken down from the domain. When image hosters implement strict takedown or even preventive measures, offenders will discuss and recommend moving away to other domains (Web-IQ, 2020; Kokolaki et al., 2020). Currently, CSAM can often be found on image hosting websites; however, this can change over time (Web-IQ, 2020).

3.1 CSAM on the Internet

To understand how CSAM is hosted, basic knowledge of how the Internet works are necessary. Therefore, this section first addresses the basic principles of how the Internet works. Then it discusses how CSAM is hosted, by which kind of companies and how it is defined in European law. At last, this section reflects on

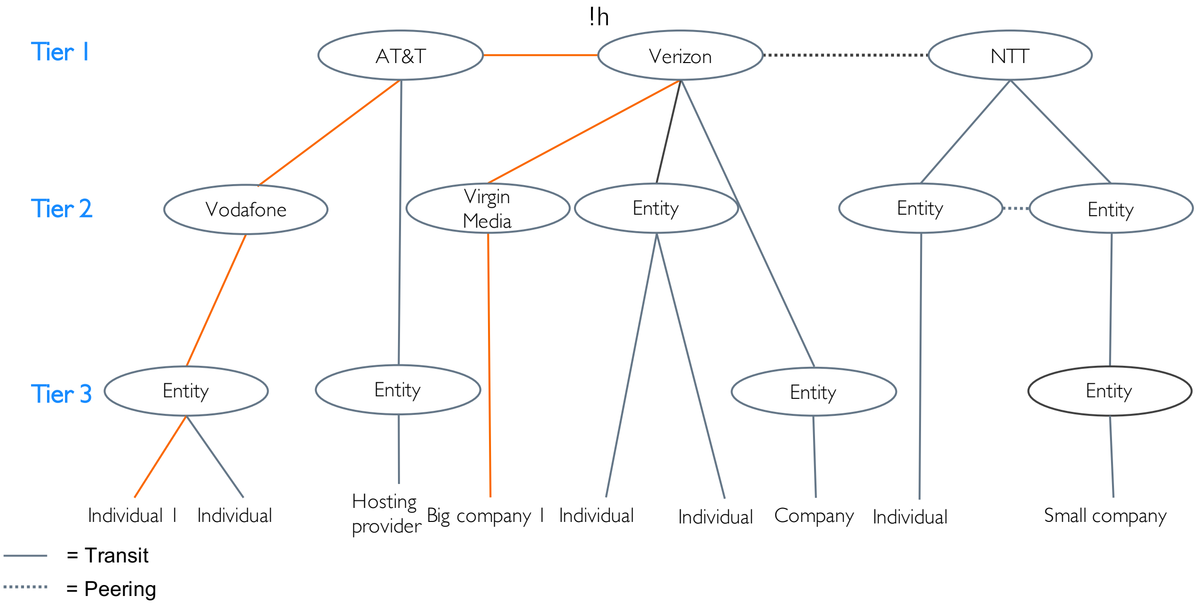

Figure 3.1: Overview Internet tiers

the classification of those companies.

Operating the Internet

The Internet consists of many independent but connects networks all around the world. The Internet infrastructure consists of, among other things, physical hardware as severs, transmission lines with types as fiber optic or microwave links and, software. Many companies, organizations, and individuals are involved in operating the Internet. All parties operating the Internet are called entities. Every entity has its network and is connected to other entities. Internet service providers (ISP's) are entities that offer access to individuals and sometimes organizations to the Internet. If one individual sends an email to another, it starts at the ISP's network of person one and ends at the ISP's network of person 2. Person 1 and person 2 are part of the network of their Internet providers. The networks of person 1 and person 2 are not necessarily connected directly. The email needs to pass through different networks before reaching the network to which person 2 is connected. Next to ISP's, other entities provide access to the Internet, like Internet access providers (IAP's)(Norton, 2008).

Data is transmitted from one point to another through the networks of different entities. Which route it takes is determined by the hierarchical structure of the Internet. The Internet hierarchy consists of three layers of entities called tiers. Tier 1 is the highest level. The networks of the tier 1 entities often have an international reach. Examples of tier 1 companies are ATT, Verizon, and NTT (Norton, 2008). Tier 2 entities are more national or regional entities, like the ISP's Vodafone or Virgin Media. Lastly, tier 3 entities are regularly much smaller and have a regional focus providing Internet access to end-users (CISCO, 2020).

An example of how data is routed through the Internet is displayed in figure 3.1, with the red line. If "Individual 1" send an email to "Big company 1". The email will pass through the network of "Internet provider 1", to the network of "Vodafone", to the network of "ATT", to the network of "Verizon", to the network of "Virgin Media", to "Big company 1". A similar path exists if "Individual 1" wants to visit the website of "Big Company 1". "Big Company 1" has stored the data from their website on their servers. Those servers are connected to the Internet through "Virgin Media". So, to get the website from "Big Company 1" to "Individual 1" the data needs to pass all intermediate companies' networks.

If an ISP or another entity is classified in a higher tier, it is an upstream entity for the entity in a lower tier. "Vodafone" is the upstream hoster of "Internet provider 1". The data exchange between entities can be done through IP transit or IP peering. With IP transit, a lower-tier company pays a company in a higher tier to pass on the data. For example, Vodafone will pay ATT to transit the data from its customer to ATT. Entities on the same tier do not have to pay each other. Consequently, peering costs less, and the route the data needs to take will also be shorter (Norton, 2008). However, to reach some networks peering on a Tier 2 level is not possible. Routed data will almost always take to shortest and quickest route, with minimal intermediate steps. Pass data from one network to another happens at Internet exchange points. A very well-known example of such a place is the AMS-IX. Data from all different networks is sent to the AMS-IX. Through the network of AMS-IX, the data is sent to the designated network to continue its journey (**?**).

All entities, annotated within bubbles in figure 3.1, have a network. All networks have an IP-address. Large entities can have multiple networks and multiple IP-addresses. When an entity has numerous IP-addresses, it is a network of IP-addresses. An ISP quickly has hundreds or thousands of IP-addresses. An IP-address is used to let other entities, like Internet providers, know they have a network. An entity also needs an AS Number (ASN). An ASN indicates the bundle/cluster of IP-addresses of the entity (Limoncelli, 2016). The cluster of IP-addresses under the ASN all have a clearly defined routing policy. In general, one company has one ASN. However, if that company has, for example, different subsidiaries and those have applied for an ASN priorly, they have multiple ASN's. Also, ISP's often have numerous ASN's. By using the BGP protocol, data is led through the Internet and finds its way from one the sender to the designation. It helps your email to get from your computer to the computer of the addressee. Companies need an IP-address and an ASN to use the BGP protocol. If an entity needs to send data, it will do that by announcing its ASN and IP-addresses of origin. All organizations in figure 3.1 within an oval have their ASN.

ASN's and IP-addresses are all assigned by Regional Internet Registries (RiR's). In Europe and the Middle East, the RiR is RIPE NCC (Réseaux IP Européens Network Coordination Centre). In the RIPE NCC WHOIS database, the allocation of IP-addresses is registered, what entity administers the network in which the IP address is located (ASN), and what the contact information is from this entity to notify abuse (**?**). Two types of IP-addresses exist, Provider Independent (PI) IP-addresses and Provider Aggregable(PA) IP-addresses. Entities with PI IP-addresses have the possibility to sub-allocate their IP-addresses to another entity. The new entity can then operate the IP-addresses from their own ASN and/or handle any abuse issues . A sub-allocation can be registered in the WHOIS database. Writing a sub-allocation can only go one layer deep (**?**). To illustrate that, let's say company A has an IP-address and sub-allocated this to company B. Company A registrants the sub-allocation in the WHOIS database. Company B will then sub-allocated it to company C. The sub-allocation of the sub-allocation cannot be registered in the WHOIS database anymore, so registration goes only one layer deep.

Concluding, the Internet exists of different elements like the Internet infrastructure of transmission lines, software, and hardware such as servers, and entities that operate networks sending and receiving data. And exchange points, like the AMS-IX, where networks of entities are connected. Entities sending data, like websites or emails through the Internet, do that from IP-addresses, which indicate their networks, and with an ASN, they announce themselves.

Classification of Internet services

The Dutch government, hotlines, and other stakeholders use different typologies for the same companies. The Dutch government often talks about hosting providers, while in reports of INHOPE, the word "ISP" come across regularly (Grapperhaus, 2020a; INHOPE, 2018).

In the e-commerce directive there is made a distinction between three types of Internet services:

1. Mere conduit
2. Caching
3. Hosting provider

Companies that offer mere conduit services only pass on data on the Internet without having any control over the content of the data. A mere conduit service can also provide Internet access (European Parliament, 2000). They do not store the data but only pass it through. This also includes all ISP's and internet companies that passing data through peering or transiting (Lodder et al., 2016). An exception to this is "over the top" communication services, which also classify as a mere conduit, like WhatsApp and Signal, who facilitate direct contact between individuals. Those companies do store data but also have no control over the content of the data (van Hoboken et al., 2020; DLA Piper, 2014). Caching services are comparable to mere conduit services focused on passing on data on the Internet. In comparison to mere conduit services is the data with caching stored for a short time with the goal to transmit the data. Hosting is legally defined as storing information provided by a recipient of the service. The storage of the data is in a hosting service the main activity. These services enable Internet users to place information on the Internet. Examples are services that put websites online or platforms on which users can upload photos and videos. For hosting CSAM, mere conduit and hosting services are the two most relevant types (van Hoboken et al., 2020).

Hosting of CSAM

Several elements are needed to get CSAM accessible on the open web. The website needs to be stored on a server. This server needs to be part of a network. This network needs to be connected to the Internet and has, therefore, an IP-address. And the network is announced an ASN when somebody wants to visit it, showed in figure 3.2.

The website, server, IP-address, and ASN are all owned by the same or different entities. The domain owner owns the domain. According to the legal definitions, a hosting provider is always the company or person storing the website information on a server provided by a recipient of the service. Therefore, hosting providers store data of third parties and not their own data. However, when users can upload their own content onto a platform, like individuals posing content on Facebook, storing this data a hosting service because the individuals are the third party. So, a company like Facebook is still a hosting provider. A company that does not own the servers on which the domain is hosted but only provides IP-address offers mere conduit service. Also, a company that only provides IP-address and announces traffic from the sever from their ASN offers mere conduit service and no hosting services (European Parlaiment, 2020).

A well-known phenomenon in the hosting sector is re-selling. Re-selling happens when hosting providers rents out server space and Internet connectivity from other hosting providers (Noroozian et al., 2019;

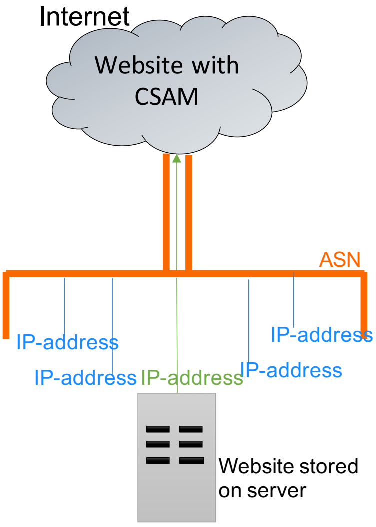

Figure 3.2: Overiew of a server, IP-address ASN and to host a website

European Parliament, 2020). For example, a domain owner wants to have its domain online but does not own servers, IP-address, or an ASN. Therefore, it rents all these means from hosting provider C. However, hosting provider C also does not own any servers, IP-address, and an ASN. Hosting Provider C will rent all that from hosting provider B. Hosting provider B does have servers but no IP-address and ASN. The hosting provider will rent the Internet connectivity from datacenter A. Datacenter A has an IP-address network and an ASN and will connect the servers of hosting provider B to their network and route their data. In this case, the services of hosting provider B and hosting provider C are both defined as hosting services as they store the information provided by a recipient of the service. Data-center C offers a mere conduit service, as they are only pass-through data without storing it.

Datacenters provide the physical space for servers and all other vital facilities like cooling systems, electricity, security, and Internet connection. As they provide IP-addresses, they have a network and will be classified as providing mere conduit services. Some companies offer both mere conduit services and hosting services (Alaerds et al., 2017). In the law there is no difference between providing access to the Internet by means of mere conduit services and peering or transiting information as a intermediate. Both provide mere conduit services.

The classification of hosting providers used by the Dutch Government

The Dutch government talks in various documents about hosting providers. Also, the TU Delft monitor writes about hosting providers. From these documents, it can be derived that companies to which IP-addresses are assigned by the RIR are addressed as hosting providers (**?**). The WHOIS database is the leading source the classify. As discussed above, legally seen an entity operating or administrating an IP-address and/or ASN does not necessarily offer hosting services. Also, entities that provide solely mere conduit services can have assigned IP-addresses. Companies providing mere conduit services are not excluded from the WHOIS database. Using a classification that is not aligned with the law can be confusing. Since "hosting provider" is the common term used by policymakers in this field to annotate companies with IP-addresses, this thesis will follow that definition. However, legally, it does not fit.

3.2 Specific challenges regulating CSAM

Governments encounter challenges while attempting to clean the Internet from CSAM. Firstly, the content is toxic. Toxic means that it is illegal to watch, share, download, or possess CSAM. The toxicity makes it difficult for companies and organizations to check if incoming reports are truly illegal and prevent over-censuring (Cohen-Almagor, 2013; Demeyer et al., 2012; DLA Piper, 2014). Also, self-initiated monitoring is not possible, as it is not allowed to keep a database with the material (Artikel 240b SR, 2020).

Additionally, in Europe, the fight against CSAM and Internet intermediates' respective roles are under intense public scrutiny. This pressure allows policymakers to change long-established rules, for example, in the field of legal liability. Much pressure can also work as a catalyst for companies to feel the urgency and adopt new policies. However, the process of change is tense. There is a risk of hasty decision-making, which leads to symptom relief or bucket-passing instead of resolving the cause. This kind of pressured change management is also known for the risk of hurting the collaborations of actors. These specific challenges are making it harder to establish a well-thought-through approach (Akdeniz, 2008).

3.3 The Dutch role in hosting CSAM

According to IWF, the Netherlands hosted 71% of the CSAM worldwide in 2019. INHOPE, in their turn, found that the Netherlands hosted 20 % of CSAM worldwide in 2019, which is equal to the percentage the US hosted in 2019 (Internation Watch Foundation, 2020; **?**). INHOPE also found that within Europe, the Netherlands hosted 79% of the CSAM in 2019 (**?**). Although there is still some disagreement about how much the Netherlands hosts precisely and considering that it is expected that we only find the tip of the iceberg if it comes to CSAM on the Internet, the Dutch Internet infrastructure is an essential facilitator of CSAM. Therefore the European Union watches the Netherlands closely and publicly expressed its dissatisfaction with their performance in the past (European Commission, 2020a).

The lousy score of the Netherlands can be partly explained by how INHOPE and IWF come to their rankings. IWF predominalty proactive searches for CSAM (Internation Watch Foundation, 2020). Currently, there is not much known about the web crawler method of IWF. Regardless, it is general knowledge that web crawlers need to be put in a position before they can start. It can be expected that the method of web crawling applied by IWF is focused on specific domains. Consequently, the reports of IWF will reflect a skewed image of the CSAM hosting environment (Westlake et al., 2017).

Another explanation of the poor performance of the Netherlands can be attributed to the magnitude of the Dutch hosting sector. The Netherlands has a favorable hosting climate, relatively cheap electricity, benign taxes, and maybe the most crucial fast Internet. The Netherlands is through TAT-14, a transatlantic communication cable connected with the US, France, Germany, and Denmark. TAT-14 provides an immediate connection between the five countries and serves as the connection between the US, Europe, and parts of the middle east and Asia (Alaerds et al., 2017). This is also why the Netherlands, Germany, and France are significant powers in the hosting sector. However, this does not explain why the Netherlands' performance is worse than France or Germany).

Furthermore, it is unexplained why (Lone et al., 2020) detected a significant difference in the level of abuse that hosting providers in the Netherlands experience. Just five hosters are responsible for 98% of the hosted CSAM in 2019 and 2020. From which NForce hosted around 82% of the total reported CSAM in the Netherlands.

Tajalizadehkhoob et al. (2018) found that for general abuse, 84 percent of the volume can be explained with structural properties such as the number of hosted domains and number of IP-address. Furthermore, are the price level, the popularity of hosted sites, and the prevalence of popular management systems also significant explanatory factors. Possibly those explanatory factors can also be applied to hosting providers regarding CSAM (Tajalizadehkhoob et al., 2018).

3.4 The Dutch approach in fighting CSAM

Already in 1995, the Netherlands declared the fight against CSAM on the Internet. That year the Internet industry established the first CSAM Internet hotline in the world to fight the material online (EOKM, 2020). Other states followed this example, and quickly after that, in 1999, INHOPE, the international umbrella organization of hotline's was founded (INHOPE, 2020b). The national hotlines and INHOPE were the first building blocks of the global CSAM notice-and-takedown. The years after the Netherlands continued its battle, the latest move is the renewed program against CSAM of the Dutch government. The program is executed by the Ministry of Jand the Ministry of EZK.

Renewed program against CSAM

This program develops around three policy lines:

1. Intensifying prevention: focused on victims, offenders of abuse, and downloaders;
2. Cleaning the Internet of CSAM: Public-private collaboration (PPC) and the introduction of a regulatory approach;
3. Strengthen the investigative system (Grapperhaus, 2018b)

Policy lines two and three aimed at having a direct effect on the victims. The first policy line of prevention is a long-term investment. It is always hard to see the immediate results of prevention. Prevention shows an effect after a long-time and can be influenced by many other factors. Borders are blurred online, prevention in the Netherlands will not be satisfactory to tackle the problem adequately (Holt et al., 2020). The third policy line aims to strengthen law enforcement to save victims and prosecute offenders. In the past years, more money is invested in the police force and technology, helping save victims, find offenders, and reveal proof to have offenders prosecuted. However, the Internet is flooded with the material; most of the material is old and non-Dutch. The police force is limited in capacity and focuses on not solving cases instead of going after uploaders and downloaders of known CSAM. Furthermore, are the police bounded to jurisdictional borders. Although the Dutch forces work closely with many international forces, they cannot stop the inflow of material all around the world completely (Grapperhaus, 2018b).

Government policies

The second policy line aims to clean the Internet of known CSAM and prevent it from being uploaded. In this thesis, the second policy line will be referred to as "government policies". It is a more pragmatic approach to the problem in which downloader or sharing offenders will not be prosecuted, but the Internet is cleaned. Cleaning the Internet of CSAM will stop re-victimizing children and go against for the International inflow of material (Grapperhaus, 2018b). Cleaning the Internet of CSAM is split up into two main components: (1) the PPC and (2) a regulatory approach. The Ministry of Jand the Ministry of EZK established the PPC in 2018. The PPC is a working group consisting of all relevant Dutch partners to clean the Internet from known CSAM. Included in PPC were, among others: representatives of the hosting sector, large ICT-companies, EOKM, TBKK, and academic representatives. The government policies consist of four pillars:

1. Transparency;
2. Self-regulation;
3. Framework for action;
4. Regulatory approach (Grapperhaus, 2018b).

Transprancy
The first pillar aims to provide insight into hosting providers' performance concerning hosting and taking down CSAM. The government intended to develop a monitor with which hosting providers could benchmark themselves. However, the Dutch Parliament asked the minister to name-and-shame the hosting providers that are not cooperating in the NTD mechanism (Oosten and Buitenweg, 2018). The nature of the instrument changed from self-regulatory to co-regulatory. TU Delft developed an independent monitor which maps how many URLs with CSAM at which Dutch hosting provider and how fast the hosters take the URLs down (Grapperhaus, 2018a). The results are based on data provided by EOKM.

The first results were presented to the minister in June 2020 but not made public. After receiving the results, the Ministry of J& V sent out warning letters to the 17 hosters TU Delft identified. The letter was both a warning as a call for action. Simultaneously, sending the letters, the Minister of Jturned around an imaginary hourglass running until the 1st of September of 2020. The hosting providers got a chance to take measures to reduce the number of reports of child pornography and to ensure that they remove the images within 24 hours of being reported (Grapperhaus, 2020b).

In September, TU Delft delivered a new report, with a more elaborate analysis of the hosters' performance. The Minister of J&V and the Secretary of State of the Ministry of EZK sent the TU Delft monitor report to the Dutch House of Representatives with a letter. The letter wrote that there was no question of a widely indifferent or non-responsive hosting sector in the Netherlands. By making the report public, the government answered the House of Representatives' request to "name" the companies. The government did not shame any company in the letter. However, the letter expressed concerns about two hosting providers. The TU Delft report was not convincing as to whether these two parties were actually participating in the joint action to tackle online child sexual abuse (Grapperhaus, 2020a).

The TU Delft will continue to monitor, and more reports will follow in the future. The government attempts to ensure that this monitor will runs as long as necessary Grapperhaus (2020a).

Selfregulation
The hosting section shapes the self-regulation pillar. The main element in the self-regulation is the Notice-and-Takedown (NTD) mechanism and agreements to it. A Code-of-Conduct (CoC) for the NTD did already existed. As part of the PPC, the industry organizations added an addendum to the CoC. This CoC included, among other things, a 24-hour takedown norm and acknowledging EOKM as a trusted flagger. Hosting providers receiving notification of CSAM should take it down within 24-hours (Noticeandtakedown.nl, 2018a). The umbrella organizations of the hosting sector (NLDigital, ISP Connect, DINL, DHPA, and NL Connect) required implementing this procedure by all members (Noticeandtakedown.nl,

2018a).

Framework for action
The Dutch government is pressuring the hosting providers to host lest CSAM and take it down quicker. In the end, not the effort counts but the results (Grapperhaus, 2020a). To help the PPC provides a framework for action to companies that receive notifications about CSAM (**?**). The framework of action's most prominent instrument is the HashCheckService, provided by EOKM and the Dutch police. Companies can check the content on their services with a database with hashes of CSAM content. A hash a digital fingerprint for content. With the HCS, companies can clean their servers. The technical system is developed and maintained by the Internet company WEB-IQ (Grapperhaus, 2020b).

The hash database includes more than 1.4 million images. The HCS was already provided in 2019, but after the warning letters sent in June 2020, the was a steep increase in companies using the HCS. More companies connected to the HCS, and in September 2020 already 18.2 billion images were checked, from which 7.4 million matched with CSAM (Grapperhaus, 2020a). Further, to support the NTD mechanism, the Ministry of J & V subsidies the EOKM (Grapperhaus, 2018c; Tweede Kamer, 2018).

Regulatory approach
The three policies named above are aimed to get a better overview of where CSAM is hosted and get CSAM better and quicker of the open web. To ensure implementation of the instruments and compliance to set norms, the government wanted a big stick. The government is introducing administrative enforcement measures targeting companies that are meticulous in cleaning their servers of CSAM (Grapperhaus, 2019b). A regulator will be established, which is mandated under administrative law to issue fines to companies exceeding the 24 hours takedown time norm after receiving a report (Steur et al., 2019).

In the future, the government can assign more tasks to this administrative body. Other activities the government has named to study if they are appropriate to allocate are: continuing the TU Delft monitor, keeping close contact with the industry, proactive searching on the Internet, and regulating a Duty of Care (Grapperhaus, 2020a). The administrative law will be put in consultation somewhere in February.

4

The working of Notice-and-Takedown mechanisms

In this chapter, the working of the Notice-and-Takedown (NTD) mechanism is discussed. In the first section, the overall structure and working of the NTD mechanism are discussed. Further, are the roles and incentives of stakeholders in the NTD discussed. Then the NTD mechanism and information sharing in the Netherlands are described. The second section zooms in on the application of NTD mechanism for illegal content. Again, the structure and working of is described. Further, does the section reflects on the regulatory framework around illegal content NTD mechanisms. Three cases are discussed to show the differences and illustrate how NTD mechanisms for illegal content work. At last, a few challenges of NTD mechanisms of illegal content are noted. The CSAM NTD mechanism is discussed in the third section. Further, is the Dutch CSAM NTD mechanism displayed. Also, this section reflects on the regulatory framework, structure, roles, and challenges. At last, a knowledge gap is formulated.

4.1 The working of NTD mechanisms

The Notice-and-take down mechanism is originally a self-regulation instrument defining the process of detecting abuse on the Internet, notifying the affected or responsible organization, and act upon the notification (Anti Abuse Netwerk (AAN), 2020; Noticeandtakedown.nl, 2018b). The NTD mechanism falls within the broader mechanism of sharing abuse data. Within the NTD mechanism and information sharing, three types of abuse are processed: abuse of technologies, illegal/harmful content, and the leakage of personal data (Anti Abuse Netwerk (AAN), 2020). Within the abuse reporting mechanism, Jhaveri et al. (2017) and the Anti Abuse Netwerk (AAN) (2020) distinguishes the roles of 1. Detector, 2. Aggregator/Reporter, and 3. Receiver are distinguished, see figure 4.1. The detector finds abuse on the Internet and provides those as notifications to another organization in the NTD mechanism. The aggregator/reporter receives notifications, forwards those to other organizations in the NTD, and have the possibility to duplication, enrichment, or/and deduplication notifications before forwarding them. The receiver is the destination of the notifications and can act upon the notification by decreasing, eliminating the abuse, or accepting the risk indicated in the notification. NTD mechanism consists of international and national information flow (Anti Abuse Netwerk (AAN), 2020). The organizations involved in the NTD mechanism and the methods used to detect material are dependent on the type of abuse. In essence, the actions of the receiver and all other roles are voluntary. Within the NTD mechanism, the detector's goal and report are always to take down the content. However, the receiver can decide themselves respond to this request (Van Hoboken et al., 2018; van Hoboken et al., 2020).

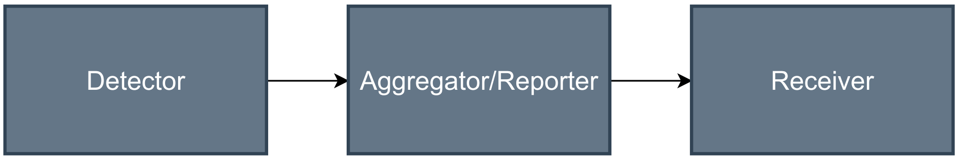

Figure 4.1: Abuse NTD mechansim

Detecting can be done by individuals who come across it, (non-governmental) organizations who actively seek for abuse, hosting providers self or law enforcement agencies (Moore and Clayton, 2009a; Jhaveri et al., 2017). Organizations, both governmental and non-profit, generally aggregate abuse. Also, specialized organizations that focus on one type of abuse, like EOKM, act as aggregators. These kinds of organizations also report abuse to hosting providers or other Internet companies. Depending on the report and which organization can be identified, Internet companies such as hosting providers, Internet access providers, Internet companies providing mere conduit services, or ISP's are contacted. Tajalizadehkhoob et al. (2016, 2017); Asghari et al. (2015) write that for web-based abuse generally hosting providers receive takedown requests. Companies receiving and takedown requests can sometimes takedown the abuse immediately. Other times, they need to pass the abuse report on to their customers to take it down (Jhaveri et al., 2017; Anti Abuse Netwerk (AAN), 2020). The hosting providers are identified by looking up the IP-address from which the abuse is hosted in the WHOIS databases, often from the RiR. For other cases in which a domain or an individual is searched, the registry or ISP is contacted. Sometimes registrars are approached as an escalation step.

There are a lot of different types of abuse online. In general, the set-up of the NTD mechanism is similar for all types of abuse. However, the involved organizations and exact processes differ for every type of abuse. Which organizations are involved dependent on which stakeholders are affected by the type of abuse and the characteristics of the abuse. For example, financial institutions are interested in taking down fake websites of themselves, and an NGO representing artists focuses on taking down content that violates copyright infringement laws. Furthermore, our cybersecurity companies are also sometimes involved. They have a good overview and the last intel about abuse, especially cybercrime. Security companies use this knowledge to offer security services to make a profit (Jhaveri et al., 2017).

Motivation of involved actors

The underlying incentives of the organizations and companies determine which actors participate in abuse specific NTD mechanism. Roughly the five categories of actors involved in the NTD mechanism are private-sector companies, non-governmental agencies (NGOs), public communities, and individuals. Those actors can have different motivations: moral duty, indirect financial harm, direct financial harm, political pressure, legal liability, the fear for government regulation, and the opportunity to exchange valuable data. Although the NTD mechanism is originally a self-regulatory instrument of the Internet sector, the participation of Law Enforcement Agencies (LEA's) and governments are observed in some cases.

Non-governmental organizations (NGOs) take part in the NTD mechanism in several ways. Their role in the NTD mechanism is closely affiliated with their mission. Regularly NGOs act in the interest of a group that experiences difficulties representing themselves in the NTD mechanism. An example is foundation

Brein, a Dutch NGO which strives for an Internet free of copyright infringement. They act on behalf of violated artists issue takedown orders on behalf of them (Lodder et al., 2016; DLA Piper, 2014).

Private companies can have multiple reasons to participate in an NTD mechanism actively. Incentives to participate include: moral duty, minimizing indirect financial harm (brand or service reputation), minimizing direct financial harm (e.g., getting black-listed for Internet connection, abuse desk costs or network overloading), sharing data to get data in return or legal liability (Jhaveri et al., 2017). For example, financial institutions monitor, aggregate, and report phishing incidents in which offenders impersonate their organization because phishing e-mails in which financial institutions are impersonated cause significant reputational damage and service costs to these institutions. Additionally, private companies can also be motivated by the fear of government regulation. Self-regulation gives the private companies much more power to decide how, when, and where they adhere to the NTD mechanism (Asghari et al., 2015).

Government's and LEA's can get involved in NTD mechanisms in specific cases. They are predominantly driven by societal goals, such as protecting civilians. Within the government's objectives can differ. For example, a ministry of Justice and Security pursues a just and safe society, while a ministry of Economic affairs aims to have a healthy and flourishing economy (Schillemans, 2013). Notable is that under current European law, the e-commerce directive, intermediates are not liable for what was happening on their servers if they are not aware of these activities. When receiving a takedown request, the companies are made aware of the content they facilitate and should act upon it. There is, however, a difference between which actions are expected from companies facilitating illegal content of cyber abuse with mere conduit services or hosting services. Companies offering the latter have a greater responsibility to respond swiftly. If not, they are liable. Companies not following takedown requests can therefore be held liable. However, in practice, it is rather hard to prove that companies did not respond swiftly, when they facilitate abuse through mere conduit services (European Parlaiment, 2020).

The integral Dutch NTD mechanism

The Dutch coalition AAN (Anti Abuse Network) is a network of parties committed to fighting against online abuse. AAN mapped the Dutch information sharing mechanism, the complete map can be found in Appendix C. In the map, three main zoned in the NTD mechanism are distinguished: Generation, Distribution, and Resolution. In the generation phase, reports of abuse are detected. In the distribution phase, those abuse notifications are spread, and in the Resolution phase, organizations act upon the reports (**?**).

Within the integral Dutch NTD mechanism, two systems of organizations can be identified: the AS-Net and the LDS-net. The AS-Net is an outdated system established several years ago and consists of agreements between organizations independently operating IP-addresses' clusters on the Internet. A cluster of IP-addresses is also called an AS. The LDS-net is a new system of agreements between parties. The LDS is an abbreviation for the national covering system. The idea is that all relevant organizations operating in the Netherlands will be covered by this system, but that is not yet (Anti Abuse Netwerk (AAN), 2020).

Furthermore, does Anti Abuse Netwerk (AAN) (2020) observes two main barriers in the Dutch NTD mechanism. Firstly, internationally exchanging abuse reports is difficult because of the many different national laws concerning sharing data. Secondly, does the Dutch government divides information streams for organizations classified as vital and not vital. Sharing abuse information between those groups is difficult.

4.2 NTD mechanism to fight illegal content

Illegal content is a category of cyber abuse. Accordingly, NTD mechanisms are also in place for illegal content. The goal of reporting illegal content is always trying to take down the content from the Internet. Where for other forms of abuse, it is possible to determine illegality by assessing technical specifications. Illegality can only be determined for illegal content by assessing the content and sometimes content within a context. In general, that is more complex and often done manually. Logically, verifying the illegality of reported content must be done before a takedown request is issued or content is removed. Otherwise, it can lead to over-censuring, a violation of fundamental rights (Ramešová, 2020; Angelopoulos and Smet, 2016). Because checking content is more complex and crucial, the role of verifier is added to the flow diagram, see Figure **??**. The verifier assesses reported content on illegality using national law.

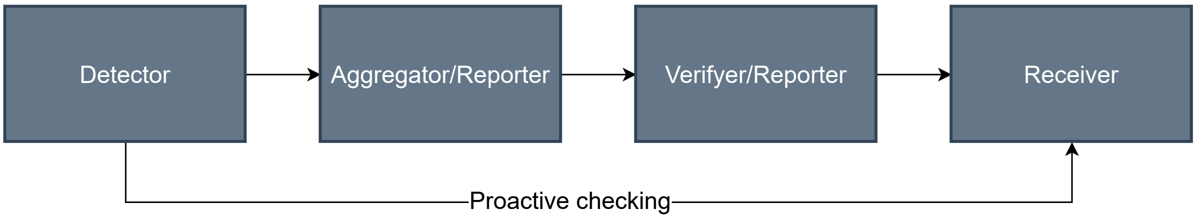

Figure 4.2: Illegal content NTD mechanism

Furthermore, in some NTD mechanisms for illegal content, an extra flow is added to the mechanism, called proactive checking. This flow goes directly from the detector to the receiver and skip's all other steps. The flow displays what happens when Internet intermediates scan their services for illegal content and remove it without other organizations' interventions (**?**Ramešová, 2020). Proactively checking is done with an automatic system that compares content on the servers with a given database. In such a database, content is saved, which is already confirmed to be illegal. For text content, phrases can be saved, and for images or videos, hashes are stored. A hash is a unique code and comparable to a fingerprint of an image or video. If an image or a video is altered, the hash will also change. AI technologies are developed that can recognize altered images. An example of such an AI technology is PhotoDNA; this AI program recognizes combinations of pixels instead of precisely the same pixels of an image or a video (Broadhurst, 2019). Proactive checking is done by the hosting provider or a domain owner. The hoster or owner will scan its servers and automatically compare all content with the database's content. When there is a match, the hoster or owner gets a notification and can take down content or block it before uploading (Grapperhaus, 2018b).

Analogous to the general abuse NTD mechanism, the actors can be Governments, Law Enforcement Agencies, private-sector companies, Non-governmental agencies (NGOs), public communities, and individuals. Also, similar to the abuse NTD mechanism, it does depend on the type of illegal content in which actors participate in the NTD mechanisms. Multiple organizations can execute one role, or sometimes multiple roles are executed by one organization (Anti Abuse Netwerk (AAN), 2020; Jhaveri et al., 2017).

Another phenomenon seen in the illegal content NTD mechanism is trusted flaggers. A trusted flagger is an organization that does not have legal authority but is considered by the industry to assess material on illegality rightfully (Çetin et al., 2016; van Hoboken et al., 2020).

Regulatory framework

In the past years, several governments intervened in the NTD mechanism of illegal content and created regulatory frameworks around it. The regulatory frameworks in western countries such as the EU, the US, Canada, and Australia are different. The regulatory frameworks apply a different definition for the NTD mechanism described above and include slightly different functionalities. Some nations have adopted the principles of a notice-and-stay down system, in which companies should prevent removed content from being re-uploaded. Another version is the notice-and-notice system, in which the content is taken down and notified to the alleged infringer (European Parliament, 2020).

Motivation of actors

The actors can have similar motivations to (actively) take part, as for participating in the abuse NTD mechanism. Incentives can be: moral duty, political pressure, indirect financial harm, direct financial harm, sharing to get data in return, or legal liability Moore and Clayton (2009b); ICMEC (2018).

There is not much research on the motivation of stakeholders within NTD mechanisms of illegal content. Hosting illegal content seems not directly to harm other clients' services, and there are also no direct for the takedown of webshops stakeholders do not experience a direct economic incentive (Hutchings et al., 2016). The incentives of the involved stakeholders in the fight against illegal content are unknown. In general, non-profit organizations are committed from the perspective of societal contribution. The governmental organization has a legal obligation to protect people and ensure economic welfare. These incentives are generalities and not proved to apply to the handling of illegal content (Carr, 2016).

Further, is the legal liability in Europe the same as for general abuse. For CSAM and terrorist content, this legal liability is changing (Ramešová, 2020).

Case studies

Copyright Infringement

Copyright infringement is illegally sharing or using content that is owned by someone else. It violates intellectual property rights and often happens with art forms like books, movies, music, or images. Some domains specifically focus on sharing so-called torrents through which infringed content is shared. The most famous example is the Pirate Bay .

The notice-and-takedown of copyright infringed material is hard. Many people make use of it, and only a small number tries to fight it. Finders are often artists (representatives) or NGOs like BREIN who search for infringed content online (Lodder et al., 2016; DLA Piper, 2014). Some NGOs do also have to gather reports of individuals. The reports are directly sent to domain owners or sometimes hosting providers.

In the EU, it is relatively easy for Internet intermediates to takedown material that violates Copywrite laws without an elaborate check. In contrast, in the US, Internet intermediates are liable for checking illegality before or after removing content (Moore and Clayton, 2009a; Wang, 2018). In the Netherlands, BREIN filed a lawsuit to enforce Internet Service Providers to block the Pirate Bay to prevent more copyright infringement. Before, BREIN sent an endless amount of takedown requests to domain owners and hosting providers, but those were unwilling to take it down voluntarily. The higher court in the Netherlands ruled that blocking a whole website is impossible but that ISP's are responsible for blocking URLs if reported by BREIN. Partly due to that ruling, BREIN became a so-named trusted flagger (**???**).

The initiatives in the area of proactive checking for copyright infringements are limited. Proactive checking is also much harder for movies because it is easier to alter the content a bit, the hash changes, and the content cannot be recognized anymore (Liong et al., 2017). Further, are Internet intermediates also not really involved in fighting this problem. In general, copyright infringement is not recognized as a very severe form of criminality. To increase the urgency felt by Internet intermediates, the European Court ruled that all member states need to declare downloading infringed content as a criminal offense (EUIPO, 2020).

Case study: Fraude: Webshop Scams

In the past years, many fake webshops have been online on the Internet. Online shoppers need to be very alert not to be scammed. During the COVID-19 crisis, criminals took their chance as an increase of fake webshops was observed (Europol, 2020). There are two types of fake webshops; fake shops that try to lure people by copying a well-established webshop or fake shops that just pretend to be a shop. In both types, shoppers lose their money when they buy something. When sites copy a well-known shop, they will often be taken down faster than the second type of fake shops because the copied shops have a strong incentive to report the fake websites and put pressure on hosting providers or ISP's (Lev-aretz, 2014).

Fake shops are almost always taken down on the rights of infringement violations. In that case, a fake webshop classifies as illegal content. Of course, this only applies to a fake webshop impersonating a well-established shop. Scams not impersonating a webshop are more a concern of individuals. The detector role is often only executed by individuals and communities. An example of such a community is Artist Against 419 (AA419), an internet community focused on identifying and closing scam web shops (Moore and Clayton, 2009a). Furthermore, national hotlines are being deployed to aggregate, verify and report notices of individuals. In the Netherlands, the Fraude Helpdesk is established to do this (Wilms, 2012).

Law enforcement agencies are also involved in prosecuting offenders possibly. However, just in a tiny percentage of the cases, they find and prosecute an offender. Because of the low chance of being caught, the willingness to report scamming is low. Victims want more than seeing that a website is taken down and therefore believe that reporting is useless (Cross, 2018).

Although a kind of proactive checking is not possible since there are billions of versions from webshops, some countries work with trademarks so customers can know which webshop is legitimate (Lev-aretz, 2014).

Terrorist content

The NTD mechanism of terrorist content is analogous to the other NTD mechanisms, based on voluntary efforts within a self-regulation framework. Platforms of several private parties, such as the Global Internet forum to Counter Terrorism, find, save, monitor, and take down illegal content (Fishman, 2019; Mirchandani, 2020). In some cases, LEA's search and detect terrorist content online for investigations. If the investigations are closed, they will issue and takedown orders (Zulkarnine et al., 2016) . Takedown orders are different from takedown requests because a takedown order issued by an LEA is often legally supported and must be followed.

The European Union (EU) is negotiating a new legal framework in which hosting providers are responsible for removing terrorist content when being notified. The proposal also includes an obligatory responsibility for hosting providers the check their services on terrorist content. It remains unclear if the obligation to check will find ground within the EU.

In some countries, including the Netherlands, this regulation will be translated to a regulator, which is able to detect, check, aggregate, and issue takedown requests. Part of the newly proposed NTD mechanism by the EU is the obligation for hosting providers to take down material within one hour. Companies offering mere conduit services are excluded from the current terrorist content legal framework (Ramešová, 2020). Sanctions for violating companies are not established yet as the EU Committee Internal Market and Consumer Protection limits the possibility for administrative bodies to have the power to issue penalties (Ramešová, 2020). Although a universal guideline on the definition of terrorist content exists, most states have their own definition of terrorist content. These different definitions can invoke problems with inter-jurisdictional takedown orders. For example, in Spain, some calls for Catalonia's independence can be terrorist content, while it is, according to Dutch national law, legal to post it online (Mitsilegas, 2021).

For terrorist content, a kind of proactive checking is also applied. An industry-led database with hashes can be freely used by domain owners and hosting providers to check their servers. With proactive checking, terrorist content can be prevented from getting uploaded and clean-up the old content from their servers (European Commission, 2016).

Challenges

The use of illegal content NTD mechanism structure has several limitations and challenges. Firstly, freedom of expression is a highly valued right in Europe. Hence, Over-censuring is a sensitive topic within Europe. Applying rigors proactive checking or taking down content without thorough assessment must be prevented. Therefore, assessing the illegality of reports according to the national law of the material demands much manual capacity. A solution to this is little proactive checking. Nonetheless, this only covers a limited number of illegal content types in which text, images, or videos are shared and only applicable for already known content. The different national definitions of what entails illegal content make it difficult to set up very effective inter-jurisdictional NTD mechanisms.

4.3 CSAM NTD mechanism

CSAM is a specific form of illegal content. Hence, the CSAM NTD mechanism structure is similar to the one described above for illegal content. However, there are some differences concerning the regulatory framework, which also affects the NTD mechanism directly. Further, are there also some more specific challenges addressed in the Dutch CSAM NTD mechanism.

Regulatory framework

The regulatory framework for the NTD CSAM mechanism in Europe is analogous to the current illegal content frameworks. Hosting providers and providers offering mere conduit services are not liable for the content they host for third persons as long as they are unaware of what the content they facilitate (European Parliament, 2000; Angelopoulos and Smet, 2016). However, receiving a notification makes them instantly aware of the content they facilitate and could make them liable. Multiple member states are researching expanding this legal liability. The Dutch government has announced a law in which hosting providers can be fined if they do not take down reported material 24 hours after receiving a notification (Grapperhaus, 2020a).

For now, self-regulation is the foundation of the CSAM NTD mechanism in Europe. In some countries, LEAs play a role in checking and issuing takedown requests (INHOPE, 2020b). The system of checking is a bit more complicated than for other forms of illegal content. Watching and downloading CSAM is illegal (**?**Artikel 240b SR, 2020). Nevertheless, watching the content is vital for assessing the illegality. Nex to that, just a few people are willing to watch this emotionally hefty material, even if it is for a good cause. Mental support and help should be available for those who do. The public prosecutor can give specific people an indemnification to watch this material to check it to take it down (Tweede Kamer, 2018). Hosting providers and their employees do not have and get an indemnification. Consequently, Internet intermediates need to trust the notifications they get without being able to check them. Therefore, the CSAM NTD mechanism is more robust than most of the other illegal content NTD's. In many countries, there is a designated hotline which aggregates, notifies, and sometimes checks reports. Those hotlines are in close contact with LEAs and are internationally connected through the umbrella organization INHOPE (INHOPE, 2020b).

Roles within the structure

In this part, it is discussed which organizations have which roles with the CSAM NTD mechanism and what their activities are in general.

Detector

The detector's role is often executed by Non-Governmental Organisations (NGOs), private companies, or individuals. At this moment, it is thought that only a minimal number of online CSAM is found (Web-IQ, 2018; ECPAT, 2015; Charalambous et al., 2016). Detecting CSAM online is complex because searching for and watching CSAM is illegal in the Netherlands as in most parts of the world. However, there are a few exceptions. Firstly, individuals are allowed to encounter CSAM by accident and then report it (Keen et al., 2020). Secondly, private companies are eligible to search for CSAM on their servers and services (McIntyre, 2013). Thirdly, Law Enforcement Agencies (LEAs) can also have been allowed to search for CSAM when it concerns investigations. At last, some NGOs are authorized by the state attorney to search for CSAM proactively. Web crawlers can be used to proactively search for CSAM (Açar, 2020). For example, the International Watch Foundation and the Cybertip.CA, the UK and Canadian CSAM hotlines are nationally authorized to search CSAM proactively. Internationally, states do also tolerated that they search for CSAM, although it violates sovereignty (Pollicino and Soldatov, 2018).

Aggregator/Reporter

An aggregator gathers reports from detectors. There are national aggregators, like EOKM and NCMEC (the US CSAM hotline), and international aggregators, like INHOPE. Reporters forward report to other aggregating organizations. INHOPE is an aggregator as it is a global network connecting different CSAM hotlines all over the world. They regulate the exchange of notifications between their members (INHOPE, 2018). Another example is EOKM, a national aggregator and gathers CSAM reports from other sources through its web form and individuals. National aggregators are simultaneously often reporters. is next to being an aggregator also a reporter as it sends Dutch CSAM reports to the industry to take the URLs down. At this moment, there are no international combined aggregators and reporters (Açar, 2020). Next to being both an aggregator and a reporter, national hotlines often also perform the role of verifier (Anchayil and Mattamana, 2010). Also, national law enforcement agencies are often classified as combined aggregators, reporters, and verifiers.

Verifier/Reporter

The verifier reviews the reported content to confirms if they are illegal according to national law. To do this, the verifier needs to evaluate the actual content instead of only looking at the technical details (e.g., file type JPG, mp4). Verifiers do also often issue takedown requests to companies. National hotlines can fulfill up to three roles of detecting, aggregating, verifying, and reporting. Also, national law enforcement agencies are often classified as combined aggregators, reporters, and verifiers(Anchayil and Mattamana, 2010). Companies that

Reciever

Receivers of CSAM takedown requests are the companies registered in WHOis databases as operators of the IP-address by which the content is hosted. The company that eventually removes CSAM is the company that is legally authorized to take down the material. The remover is the company that owns the domain or the company which owns the server on which the URL is hosted (EOKM, 2020; Anchayil and Mattamana, 2010). Depending on the services a hosting provider offers, they can take it down themselves, or they need to inform their client. It is expected that hosting providers often send a notification to their clients, sometimes directly to domain owners, and if they do not take action, they will take down a URL themselves. Sometimes their client is also not the domain owner, but there is a re-seller construction. In that way, the report needs to be forwarded until it reaches the client. However, in the Netherlands and most other countries, responsibility is put on the hosting providers. This because often hosting providers are registered in the WHOIS register as operators of the IP-address. In the Netherlands' case, many hosting providers are located on Dutch territory while website owners are located all around the world (Grapperhaus, 2018a).

Motivation of actors

The motivation of actors within the CSAM NTD mechanism is similar to actors' motivation within the NTD mechanism of illegal content. Actors and companies are minimally influenced by direct and indirect financial harm and more driven by moral duty.

Challenges

Within the literature, challenges of the CSAM NTD mechanism are discussed per role.

Detector

Mthembu (2012) underlines that because persons and private institutions do not have a legal responsibility to report CSAM, valuable information is missed every day. However, it is discussed by Charalambous et al. (2016) that depending solely on tipped CSAM is ineffective and time-consuming. Thus, the use of automated crawlers yields more success. However, Westlake and Bouchard (2016); Westlake et al. (2017) note that the use of web crawlers can be lead to incomplete and inaccurate data and breached sovereignty principles.

Aggregator/Reporter

Aggregators and Reports are NGOs or foundations, which makes them dependent on external funding for financial resources. Consequently, there is a limited budget for capacity and technical systems to adequately send all reports to the right organizations (Açar, 2020).

Verifyer/Reporter

CSAM reports only include URLs, and therefore checking CSAM is mainly done manually. Opening a CSAM URL is illegal in the Netherlands. The state attorney grants indemnification to people entrusted with checking CSAM reports working at hotlines or LEAs. Due to the limited budget, knowledge, and limitations of the law, capacity, and technological developments are often lacking(Açar, 2020).

Receiver

However, HPs do not have a legal obligation to delete it as the European Union and the USA have moved away from so-called legal intermediate liability (Anchayil and Mattamana, 2010). Accordingly, deleting CSAM is predominantly based on self-regulation and moral consciousness. Intermediates that are not motivated by one of these reasons will be inclined to ignore notifications (Mthembu, 2012).

Mechanism

The mechanism represents the whole process, from finding CSAM to taking it down. It annotates the collaboration of the involved parties. For an effective mechanism, self-regulation of the private sector and legal regulation in terms of liability combined with financial resources are vital elements (Akdeniz, 2008). However, even if all organizations can work effectively, for adequate functioning of the NTD mechanism, the organizations must communicate with each other successfully. The lack of universal standardization of definitions and processes are causing communication problems and hick-ups in the chain (Calcara, 2013). Also, the division of tasks due to the "toxicity" of the material makes it hard to align all organizations. Furthermore, the policy-making process around the mechanism is influenced by national governments, supranational organizations, and to some extent, sponsors of the mechanism and intergovernmental or international organizations. For example, the European Union owns power through the European Directive 2011/93. These organizations have different means, such as financial, communication, legal and, information resources to influence the mechanism.

4.4 Dutch NTD mechanism

The Dutch NTD mechanism of CSAM is not elaborately described in the literature. Non-academic documents give a first impression of what the Dutch NTD mechanism consists of. A flow diagram is constructed with annual reports, descriptions of involved organizations, documents for the Dutch parliament, and private initiatives.

The Dutch NTD mechanism exists of the standard NTD building blocks: Detector Aggregator, Verifier/Reporter, Receiver (INHOPE, 2020a). To clean the Dutch servers, the most important players in the Netherlands are EOKM, TBKK (The Dutch specialized police force on child sexual abuse), the IP-address operators, and hosting providers (Noticeandtakedown.nl, 2018a; Grapperhaus, 2020c; Coalitie AAN, 2020). The reports EOKM gets are provided by the INHOPE network, the Dutch public, and companies (EOKM, 2020). The Dutch public consists of individuals and organizations which report CSAM through the web form of EOKM to the hotline. TBKK receives reports from LEAs of countries that do not have a hotline and the US hotline NCMEC (INHOPE, 2020a; EOKM, 2016). In 4.6 the flow diagram of the Dutch NTD is shown.

The process of detecting, aggregating, and checking CSAM before it is reported to INHOPE or EOKM is strongly dependent on the country of origin (INHOPE, 2020a). Further, some flows remain unclear

Aug (2019) – Nov(2019)		**Jan(2020)-Aug(2020**	
Hosting Provider	**No of URLS**	**Hosting Provider**	**No of URLs**
NForce	19,393 (72.31%)	NForce	174,652 (93.57%)
IP Volume	5136 (19.15%)	KnownSVR	4581 (2.45%)
LeaseWeb	1013 (3.77%)	IP Volume	4420 (2.36%)
KnownSRV Ltd	752 (2.80%)	LeaseWeb	2013 (1.07%)
Others	750 (1,95%)	Others	1049 (0.56%)
Total	**26,819**	**Total**	**186,715**

Table 4.1: Number of CSAM Urls hosted by Hosting Providers (Lone et al., 2020)

Hosting Provider	**2020**	**2019**	**2018**
NForce	1	1	1
KnownSVR	2	4	
IP Volume	3	2	
LeaseWeb	4	3	5
ISPIRIA Networks	5		
Serverius Holding		5	
Incrediserve			2
Swiftwill			2
Quasi Networks			4

Table 4.2: % URLs per Hosting Provider per month 2019/2020 (Lone et al., 2020)

because of inconsistent reporting. Since January 2020 EOKM has adopted a new automatic system called SCART. From that moment on the number of takedown requests has increased significantly, see figure (Lone et al., 2020). Although there are some major fluctuations, see figure 4.5.

As discussed, the sector the included into their self-regulation that CSAM hosting providers should take down CSAM within 24 hours after it is reported.

Information flows and takedown times of hosting providers

EOKM reports in their annual report that they received in 2019 657.604 URL's. 308.430 were unique, and EOKM processed 271.783. From the 271.783 processed reports, 76% was illegal EOKM (2020). In the last years, EOKM has seen an increase in received reports. Between 2018 and 2019, this increase was 38%.

TU Delft developed a monitor to determine which hosting provider hosts how much CSAM and how fast they take it down after being notified. Table **??** shows the distribution of CSAM among hosting providers. Notable is that 98% of the hosted CSAM was between August and November 2019 hosted by five hosters and increasingly more than 99% between January and August in 2020.

Table **??** and figure 4.3 show that the top five hosting providers remains quite stable over the years. Especially since Lone et al. (2020) the IP-addresses once operated by Incrediserve and Quasi Networks are now allocated to Qausi network. The same network clusters for every hoster imply that only a cosmetic name change has been adopted and no other company changes. Furthermore, the study finds that around

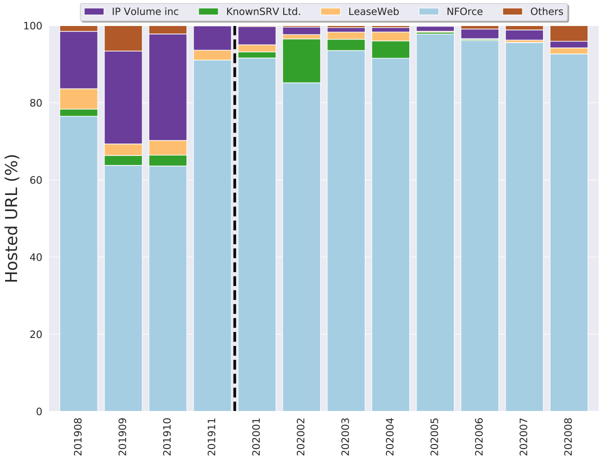

Figure 4.3: % URLs per hoster per month 2019/2020 (Lone et al., 2020)

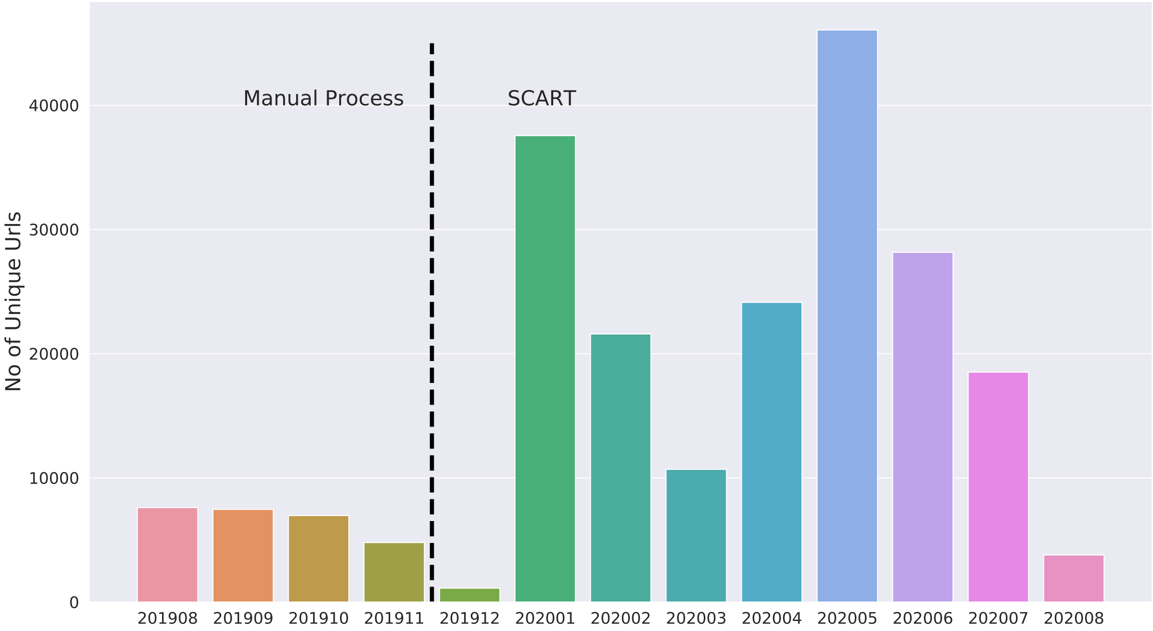

Figure 4.4: Number of URLS notified per month by EOKM (Lone et al., 2020)

84% of the reports are taken down within 24-hours. The takedown time is only measured in August. After that, it fluctuates per hosting provider.

It is also striking that the top 4 remains relatively stable as Lone et al. (2020) did not find any proof that CSAM is concentrated on a few domains. The volume of CSAM seems to switch swiftly from one platform to another.

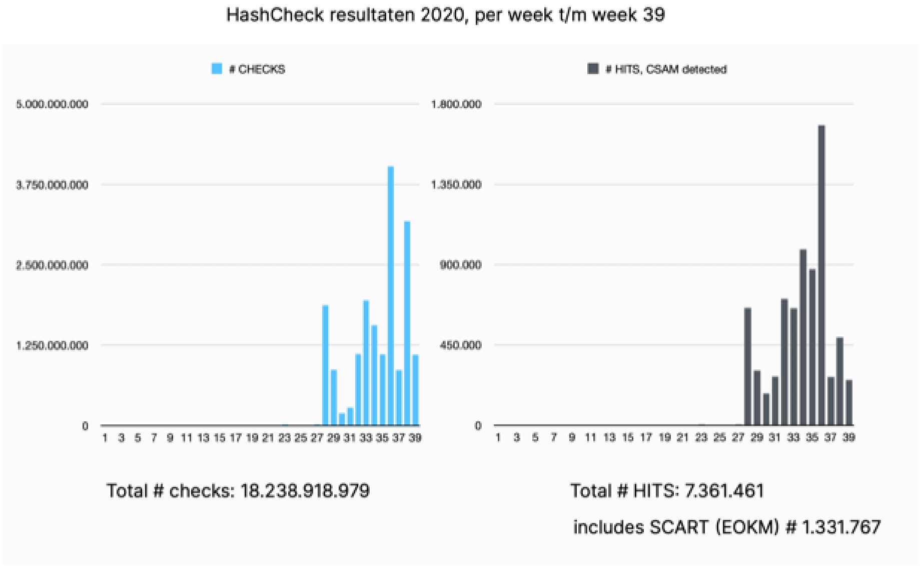

Figure 4.5: HashCheckService checked and hits until week 39 of 2020(Grapperhaus, 2020a)

The HashCheckService (HCS) is a service offered by EOKM with which companies can check if they host CSAM on their servers. Companies plug into the HCS, and the content on their servers is compared to the hash database provided by the Dutch police. If the HCS detects a match hosting provider get a notification and can take action by removing it or ignoring the notification, the flow of the HCS is shown in 4.6. Although the execution of the steps lies at the hosting provider, the process of detecting, checking, and notifying is automatic that cannot be controlled (Grapperhaus, 2019a).

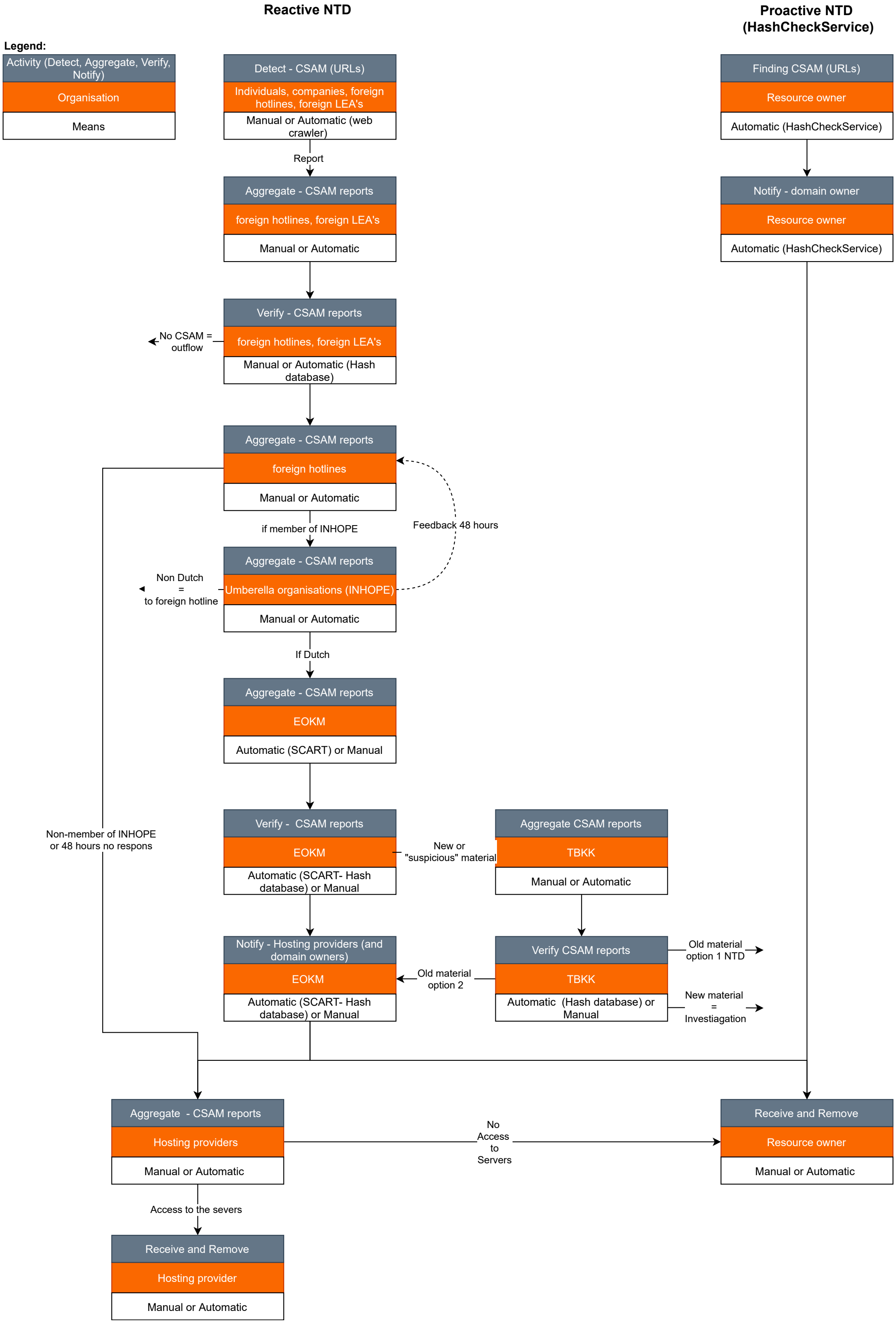

Figure 4.6: Illegal content NTD mechansim

Challenges of the Dutch CSAM NTD

In the literature, several challenges of the Dutch NTD mechanism can be found limitations of the capacity of EOKM and the police, the sloppiness of some companies, mismatching international regulations, bumpy international collaboration, and finding only the tip of the iceberg of material online.

First of all, the Police and EOKM experienced a significant increase in reports from 2013, and this increase continues (Opstelten, 2013; Blok, 2017; Grapperhaus, 2018d). For both EOKM and TBKK, this increase leads to a lack of staff capacity. TBKK needed to prioritize only present abuse situations and haves limited time to fight the spread of CSAM online (Steur et al., 2019; Opstelten, 2013). Also, EOKM struggles with the enormous amount of reports they receive. In 2019 EOKM received 657.604 reports (with duplicates) and managed to process 271.783. The total amount of FTE's grew from 3.1 to 5. However, they also saw an increase of 38% in the reported URLs. The ever-growing number of reports is difficult to tame (EOKM, 2020, 2018).

Secondly, mismatching international regulations can lead to increased workload and reporting errors. There is a global baseline that is followed internationally (INHOPE, 2018). However, countries still have different rules on top of that baseline (ICMEC, 2018). Even despite the adoption directive 2011/92/EU within the European Union, mismatching legal frameworks still exist in Europe (Kokolaki et al., 2020). An illustration is the illegality of fictional child porn. In Japan, it is not illegal, and in the Netherlands, it is. If the Japanese hotline finds this material, it will possibly mark the image as legal. EOKM never gets a notification, and a reporting error occurred. Also, the age of consent, among other elements, is different through the EU (INHOPE, 2020a; ICMEC, 2018). Further, it is also possible that some hotlines mark material as illegal, while in the Netherlands, it is not illegal. EOKM needs to double-check the reports about this kind of material to prevent over-censuring. At last, if EOKM reports to another state, and it is not illegal there. The country will not take it down, and the material is still accessible. Interesting to note is that Moore and Clayton (2009a) found that legal frameworks seem to have little effect on the take downtime speed.

Next, internationally the collaboration does not always seem adequate. INHOPE was always the umbrella organization of the hotlines. One of the main struggles is that Cybertip.ca left INHOPE in March (Lone et al., 2020). Cybertip.ca was always one of the most significant contributors to CSAM reports. Now since they left INHOPE, EOKM does not receive their reports anymore. They report directly to the Hosting providers. Therefore, it is hard for EOKM and the TUD monitor to keep an overview of hosting providers host how much (Lone et al., 2020).

Finally, a challenge is the under-reporting of CSAM. Content can only be reported as it is found, and it is only found at places where there is a search.

4.5 Knowledge gap

Based on the literature study presented in chapters 2, 3 and 4, research gaps are found. Three knowledge gaps have been identified, namely, (1) there is little research that identifies real-world execution and processes of the CSAM NTD mechanism and other instruments like the HCS, (2) the influence of stakeholders' positions and their participation in the policymaking process on CSAM government policies has not been studied, and (3) research lacks an overview of the effects of the current government policies and possible improvements to them.

Real-world execution of the CSAM NTD mechanism and affiliated instruments

Few studies describe the real-life execution of processes like the NTD-mechanism and application of instruments for proactive searching (Coalitie AAN, 2020; Noticeandtakedown.nl, 2018a; INHOPE, 2020a). Most literature discussed how systems technically work and how processes theoretically should be executed. Theoretical challenges are also addressed in the current state-of-the-art literature, such as juridical conflicts of national and international law (Demeyer et al., 2012; Anchayil and Mattamana, 2010; Steel et al., 2020). Some studies map the NTD mechanism for specific types of content. For example, Hutchings et al. (2016) has performed lengthy interviews with organizations involved in the takedown of fake websites. Their study makes an essential contribution to understanding the working of NTD mechanisms in the real world. Insights into the real-world processes are missing in the area of the CSAM NTD mechanism and affiliated instruments. Moreover, some studies reveal challenges within the CSAM NTD mechanism. Most of these studies focused on one executive role within the NTD mechanism, like detecting material, aggregating, or verifying it (Keen et al., 2020; Açar, 2020, 2017; Akdeniz, 2008; Anchayil and Mattamana, 2010; McIntyre, 2013).

Additionally, the TU Delft monitor report, annual reports of hotlines, and other documents have quantified parts of the CSAM NTD Mechanism data flows. However, no studies are found that address the integral CSAM NTD mechanism. Also, no studies combined quantitative research with qualitative research. Consequently, a thorough understanding of the NTD mechanism and the effects specific processes have on the information flows and processing times is missing. Therefore, this research focuses on mapping the detailed information flows of the NTD mechanism through performing both a quantitative and qualitative analysis.

influence of stakeholders on the (execution of) Government policies

The second gap is the lack of knowledge of how stakeholders' positions and their participation in the policymaking process influence CSAM government policies. Stakeholders are indispensable to clean the Internet from CSAM. The role of the sector and NGO's are huge in the CSAM NTD mechanism and affiliated instruments like the HCS. The research of Jhaveri et al. (2017); Asghari et al. (2015) shows stakeholders' underlying incentives to participate in the NTD mechanism of general abuse handling. A literature search revealed that it is not yet studied if the motivations of stakeholders participating in the CSAM or illegal content NTD mechanism are similar to those determined for general abuse NTD mechanisms.

Next to the stakeholders that have a role in the CSAM NTD mechanism, there are also other stakeholders with other interests in cleaning the Internet of CSAM. Examples of that type of stakeholder are The Ministry of JV, the Ministry of EZK, the European Commission, and industry representatives. Both stakeholders with an executive role and other stakeholders with interest influence the policies to clean the Internet of CSAM. Furthermore, relations between stakeholders also influence the policies' outcomes to clean the Internet of CSAM (Charalambous et al., 2016; Kokolaki et al., 2020; INHOPE, 2020a). Relations between stakeholders is correlated to the responsibility the stakeholders have. Different stakeholders take different responsibilities, as discussed in some studies (ICMEC, 2018). Other research defined why some responsibilities should not lay at specific stakeholders (Truyens and Van Eecke, 2016). However, a knowledge gap exists on how the perceived responsibilities and the stakeholders' position influence the way they participate in the policymaking process. Therefore, it is also uncertain how the participation of the stakeholders affects the establishment, implementation, and execution of government policies regarding CSAM. This research aims to reveal the influence of stakeholder's position, responsibility, and participation in government policies through the conduction of interviews.

Improvements to the Government policies

The final knowledge gap is an overview of the effects of the current government policies and possible improvements. Governments around the world are struggling with regulating illegal content and CSAM online (Holt et al., 2020). Involved organizations such as hotlines and internet companies have provided and implement several instruments, measures and policies to clean the Internet of CSAM in the past years. However, little research is done about the effects of these policies.

Moreover, there are studies that discuss possible improvements to the fight against CSAM (International Centre for Missing & Exploited Children, 2017; Açar, 2020; INHOPE, 2018). However, the relevance of the improvements is not yet investigated. An overview of multiple possibilities of improvements is lacking. Consequently, studies weighing and discussing different improvements are missing. Therefore, it is difficult for governments to decide which improvements they should invest in cleaning the Internet for CSAM. This study will provide an overview of the effects of the current government policies and improvements.

5

Methodology

The following research sub-questions were formulated based on the identified knowledge gap and keeping in kinder the intent of the Ministry of Jto use the research results to support their policymaking efforts:

How can the Dutch government policies to clean the Internet from Child Sexual Abuse Material (CSAM) be improved?

In the first section of this chapter, the mixed methods approach for this study is introduced, and sub-questions are formulated. The second and third sections elaborate on the methods which are applied per sub-question. The third section explains why the theory of the rounds model of Teisman (2000) is used in this study. Additionally, an actor analysis is included in the qualitative methodology. In the following sections, the interview protocols, qualitative data processing, data management, and research ethics are discussed.

5.1 Choice of approach

A mixed-methods approach is appropriate to answer the main research question (Morgan, 2017). Mixed methods are often used in political-themed studies, in which quantitative analysis is lacking in explaining behavior, and qualitative analysis is not able to indicate the relevance of findings (King et al., 1995). That is precisely the case with this study goal. The available quantitative data is limited and only roughly quantifies the performance of the government policies. Qualitative data is also missing and should be weighted with quantitative findings. A mixed-methods approach will be used to gain depth into the topic and put the results in perspective (Anderson et al., 2011; Buckley, 2015).

Because qualitative data is predominantly lacking in existing studies, the main research activity will be to gather and analyze qualitative data. The qualitative analysis will be used to reveal relevant stakeholders, their positions, how they participate in the policymaking process, how they evaluate the government policies, and what they believe are the most significant improvements to the system (Cronholm and Hjalmarsson, 2011). The quantitative analysis aims to complement the already existing data and provide more quantitative insights into the government policies.

The combination of quantitative and qualitative results will provide the opportunity to cross-validate (Jick, 1979). A challenge of this approach is that using two or multiple methods can be time-consuming and is challenging to generate valid results in both analyses. Furthermore, a limitation is that quantitative and qualitative methods are often based on different theories or paradigms, leading to a misalignment in the research (Brannen and Moss, 2012).

Based on the research approach presented above, the following research sub-questions are identified to answer the main research question:

1. How does the Dutch NTD mechanism and the HashCheckService look like in terms of processes, information flows, and processing times per organization?

2. Who are the relevant stakeholders, and what is their position regarding the government policies to clean the Internet of CSAM?

3. How do the relevant stakeholders participate in the policymaking process?

4. How do the stakeholders evaluate the current government policies?

5. What are the most relevant policy improvements suggested by the stakeholders?

5.2 Quantitative method

The quantitative analysis will partly answer the first sub-question. As there is no open query data available on this topic, data will be collected from involved organizations. The data is provided by EOKM, INHOPE, IWF, and the Canadian hotline. The data of EOKM includes information about the internal report, processing times, and the in- and out-flow of reports at the hotline from the 23rd of October 2020 to the 21st of December 2020. EOKM also provided data about the the number of checks and hots of the HCS from week 47 2020 to week 6, and when companies plugged in to the HCS. Researcher at the TU Delft ir. Q. B. Lone helped to analyze the data provided by EOKM. INHOPE provided data on the number of reports sent to the Netherlands per hotline in 2018, 2019, and 2020. The data of IWF includes information about the amount of sent reports from IWF to the Netherlands from 2019 and partly 2020.

The Canadian hotline data consists of all sent takedown requests to Dutch companies from January 2018 to January 2021. Every data entry is a takedown request and indicated the date it was sent, the company it was sent to, the hashed URL, and the hash of the content. Data entries from the same company, content hash, and URL hash were assigned to one label. The takedown time was then calculated by determining the number of days between the first takedown request and the last takedown request. When a label occurred only once in the database, it was assumed that the content was taken down within 24 hours. The data is also used to analyze how much CSAM providers are hosted, based on the number of unique entries excluding duplicates.

5.3 Qualitative method

This section touches upon all elements to understand which decisions are made for the qualitative analysis. Firstly, the choice for semi-structured interviews is explained. Secondly, the theory of the rounds model is described. The third part explains how the interviews are designed and conducted. The interview protocol, the data processing, and the participant recruitment of the interviews are included in the third part. Then in the fourth part, the stakeholder selection is made with the help of an actor analysis. At last, a description of the data management and research ethics is given.

Choice for semi-structured interviews

The qualitative part of the research answers sub-question 1 partly, 2, 3, 4, and 5 through an interview methodology. Interviews are perfect for studies with an exploratory character (Sekaran and Bougie, 2016). Contrary to surveys, the application of open questions and the flexibility of interviews enables the opportunity to get a deep understanding of the research topic (Emans, 2004).

Semi-structured interviews are most suitable to gather data to answer the sub-questions. Three types of interviews can be distinguished: (1) unstructured, (2) semi-structured, and (3) structured. There is no real interview protocol in unstructured interviews, which makes it suitable for an open exploration of the topic but makes it hard to compare answers. Structured interviews are quite the opposite. Here is the interviewer expected to stick to a strict protocol. The strict protocol makes it easy to compare answers but excludes the possibility of gathering new insights. Semi-structured interviews provide the opportunity to compare the gathered data but still collect new insights through the interviews (Adams, 2015; Horton et al., 2004). An interview protocol of semi-structured interviews consists of structured open questions and leaves space for the interviewer to differ from the protocol (Wilson, 2014).

A challenge of using semi-structured interviews is to design an interview guide that does not steer participants while keeping the quality of the answers consistent enough to compare them (Kallio et al., 2016). Another challenge of using semi-structured interviews is that it is very time-consuming. When studying a large and diverse group, it is hard to get a representative population sample (Adams, 2015).

Theoretical basis: the rounds model

Multiple theories explain the processes around policymaking, the network approach seems most appropriate for this study. The network approach is relatively and is based on the belief that society exists of open and closed networks (Haans, 2008). Policymaking processes form around problems. A network of stakeholders with inter-dependencies and limited resources forms around problems. Stakeholders behave according to their social capabilities caused by interaction patterns with the stakeholders in the network. The social interactions are determined by the social structures (Jacobs, 1993). Jacobs (1993) states that an actor is capable of strategically change the social structures. In conclusion, the policy-arena is very dynamic; actors act according to institutions and are also capable of changing those. In contrast, in a process management approach, policymaking is built on the control of one central actor, which manages the process in line with core elements as transparency, goals, progress, and the protection of values (De Bruijn et al., 1998). The PPC in charge of the government policies reflects the network society and constitutes a new policymaking way. The conflicting interest of stakeholders in partnership decision-making causes dynamic, messy, and unpredictable policy processes (Cohen et al., 1992). Accordingly, the network theory seems most fitting (Teisman and Klijn, 2002).

Teisman (2000) discusses three models to understand the policymaking processes with networks: (1) The phase model (Crosby and John, 1992) , (2) the stream model (Cohen et al., 1992), (Kingdon, 1984) and (3) his own rounds model. The theory of the round model will be used to set-up the interviews and analyze the results.

Phase model

The phase model is a simple representation of the different stages in a policymaking process. The phase model includes at least the policy formation, policy adoption, and policy implementation phase. Every phase constitutes of actors and activities. Characterizing for the phase model is that in general, every phase is led by one problem owner who determines the decision made in that stage (Teisman, 2000). However, a critique of this model is that policymaking processes are not linear in the real world. During the whole process, interactions of stakeholders determine goals and effort (Teisman, 1992).

Stream model

The streams model consists of three "streams": the problem stream, the solution stream, and the participant stream. The model of (King et al., 1995) resolves around one policy area's agenda-setting and policymaking process. The policymaking processes are executed in an inter-organizational setting. A policy window opens when the three streams meet. At that moment in time, decisions can be made, and actions can be taken. It is a coincidence when the three streams come together (Cohen et al., 1992). Contrary to the phase model, this does not happen linearly but crisscross in time Teisman (1992). Although this model recognizes the networks exist, it is predominately based on institutional and hierarchical context (King et al., 1995).

Rounds model

The rounds model sees the policymaking process as a joint effort of stakeholders. Not one stakeholder is capable of steering the whole process. All stakeholders are interdependent and have limited resources. The policymaking process in the rounds model is split up into rounds. In each round, individual stakeholders can make decisions that will determine the direction of the process partly. In the end, all those individual decisions determine the policies and the execution of those. Teisman (2000) explains that decisions are made based on internal and external factors of stakeholders. Firstly, all actors' base decisions on their underlying belief system, consisting of ambition, a frame of reference, and supportive facts. The ambition is what a stakeholder would like to achieve regarding the problem. The frame of reference is how the stakeholder perceives the problem. Furthermore, the supportive facts are observations and data used to support their frame of reference (Teisman et al., 2009). Besides the actors' underlying belief system, the (in)formal relations they hold with other actors also influence their decisions.

The rounds model seems to reflects the policymaking process around the government policies quite well. Therefore, the theory of the rounds model will be used to set-up the interview protocols and analyze the participants' answers.

The Public-Private partnership is an excellent example of the shift from a government to a governance approach (Teisman and Klijn, 2002). The theory behind the rounds model can be used to determine all stakeholders' position and commitment to the government policies and see how they participate in the partnership. In line with the rounds model, (Teisman, 2000) defined four different actor strategies along two axes. Table 5.1 displays the different actor strategies. The strategy's focus is either autonomous perpetuation, in which the stakeholders try to defend their position, role, and policies, or interactive, in which stakeholders actively try to collaborate to reach their goals. Secondly, the stakeholders can have an offensive or reactive strategy. An offensive strategy implies that a stakeholder actively pursues its goals. Stakeholders will often adopt an offensive strategy if they have a great interest and influence in the policymaking process. Stakeholders applying a reactive strategy respond to the initiatives other stakeholders introduce but do not initiate initiatives themselves.

	Autonomous perpetuation	Interactive strategies
Offensive strategy	The stakeholder is very assertive in initiating its plans	The actor strives for ambitious plans in collaboration with others
Reactive strategy	The stakeholder tries to fend off the plans of others	The stakeholder accepts other plans and tries to find opportunities

Table 5.1: Possible stakeholder strategies

Interview methodology

Figure 5.1 provides an overview of the followed interview process consisting of 7 stages. At first, the background of the problem is studied by means of literature and reports 2, 3 and 4. Secondly, the goals of the qualitative study are formulated. During this step, it is determined which information should be gathered with the interviews. In the third step, the interview questions are formulated using the background study, interview goals, and the rounds model. Fourthly, interview participants are recruited. Part of the recruitment process is performing an actor analysis to determine the relevant stakeholders. Designing the interview protocols and the selection of stakeholders is an iterative process. To create a good interview protocol, they are tested and improved before the first interview. After establishing the protocols, the interview was conducted online due to the COVID-19 crisis. The interviews were recorded and then transcribed. Most interviews were conducted in Dutch and translated into English by the interviewer. Those results are analyzed and inserted into the research in chapter 6 and 7.

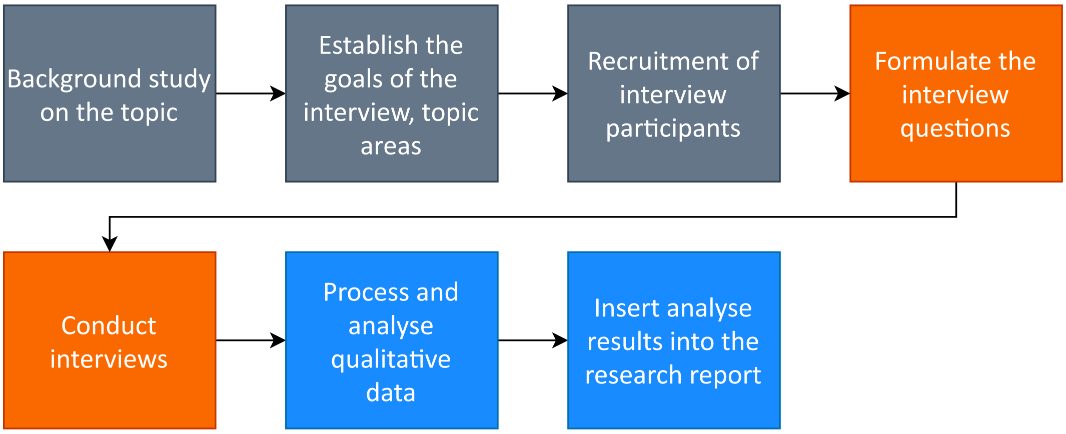
Background study on the topic
Establish the goals of the interview, topic areas
Recruitment of interview participants
Formulate the interview questions
Conduct interviews
Process and analyse qualitative data
Insert analyse results into the research report

Figure 5.1: Interview process

Stakeholder selection and recruiting

An initial actor-network scan is performed to select which stakeholders are relevant to this study. An initial actor-network scan helps to extract the influential and interested actors (Cunningham et al., 2018). The data sources were open Internet entries, experts of the Ministry of J&V and TU Delft, and my knowledge. For some stakeholders, the initial information was hard to find. Therefore, the results of the analysis are not necessarily accurate. Nevertheless, the initial actor-network scan provides a good first insight into the policy arena. Firstly, a complete list of all actors that are in some way involved is drawn up. A brief description of these actors, their strategic objectives, problem-specific objectives, and interest in the problem is formulated. Secondly, the first expectation of the actor's resources and their level of power is described. Both tables can be found in Appendix A. Those overviews are then used to create a power-interest diagram, as shown in figure 5.2.

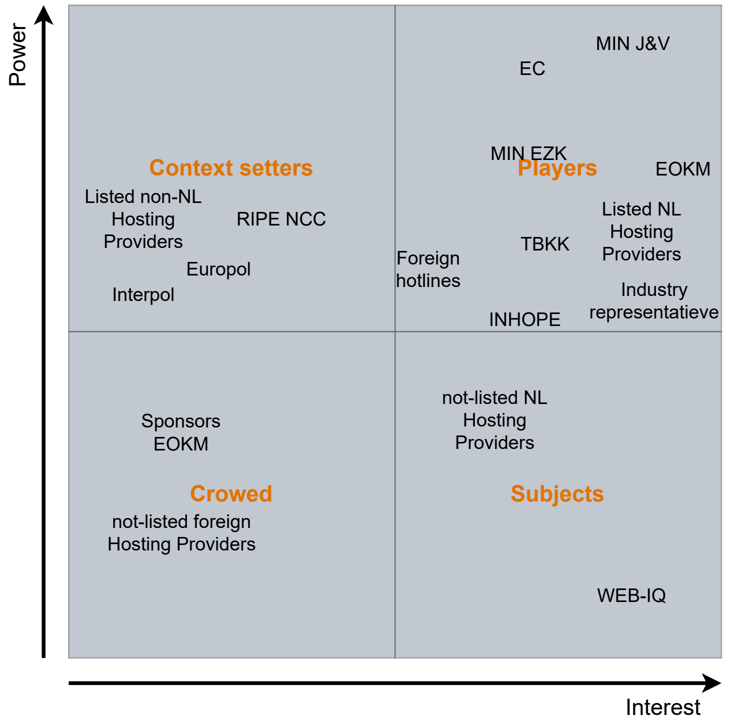

Figure 5.2: Power-Interest Grid

Based on this power-interest grid, all stakeholders classifying as players are selected. An expert of TU Delft recommended including RIPE NCC into the sample because of their potentially important role. RIPE NCC is the only context setter included in the sample. The high-power actors are selected as the government aims to all relevant stakeholders in the PPC. There are two types of stakeholders. First, stakeholders that perform tasks in the NTD-mechanism and affiliated instruments. Those executive stakeholders are hosting providers, INHOPE, TBKK, EOKM, and foreign hotlines. Second, stakeholders that are solely involved in facilitating and supporting activities such as the Ministry of J, the Ministry of EZK, the EC, and the Industry representatives. Those stakeholders do not have a role in the NTD mechanism but can form the policies through regulations, agreements, financial resources, and so on.

The number of stakeholders is based on assuring the representativity of the interviewees (Horton et al., 2004). However, the time limit of the study limited the total number of interviews. The number of participants per stakeholder is chosen to guarantee representativity as much as possible. At least one interviewee is conducted per stakeholder. The number of interviews per stakeholders is displayed in table 5.2.

For every stakeholder with an executive role in the NTD-mechanism or affiliated instrument and takes place in the PPC, at least two participants are recruited. Moreover, most of the stakeholders represent themselves and are not part of a bigger group. There is just one Ministry of J&V, one Ministry of EZK, and so on. However, hosting providers and hotlines are part of a bigger group. Due to time limitations, it

Overview stakeholder interviews		
Stakeholders	**Number of interviews**	**Executive or Policy role**
Hosting providers	Total of 6 interviews with 6 different companies	Executive role
Hotlines: -Dutch (EOKM) -Canadian (Cybertip.CA) -French, (Point de Contact) -UK, (IWF) -US, (NCMEC)	Total of 6 interviews - EOKM: 2x - Cybertip.CA: 1x - Point de Contact: 1x - IWF: 1x - NCMEC: 1x (6 people)	Executive role. The Dutch hotline is an exception as they take place in the PPC
Industry representatives	Total of 3 interviews with 3 different representatives, of 2 different organisations	Facilitating role
Dutch police, special force CSA (TBKK)	2 interviews	Executive role. TBKK takes place in the PPC
The ministry of J&V	1 interview	Facilitating role
The ministry of EZK	1 interview	Facilitating role
The European Commission, DG HOME	1 interview	Facilitating role
INHOPE	1 interview	Facilitating role
RIPE NCC	1 interview	Facilitating role

Table 5.2: Overview of interview participants

is decided that only six interviews could be conducted from both groups. A risk is that representativity is not reached with both samples.

Different experts estimate that the Dutch hosting sector consists of up to a thousand or even up to thousands of hosting providers. The sector's magnitude is also dependent on which characteristics there are used to determine if a company is a hosting provider. It is expected that because of the wide variety and the volume of the sector, the sample is not representative. Therefore, the recruitment of hosting providers aimed at gathering a high diversity between companies is most suitable for an exploratory study. For the hosting providers' recruitment, industry representatives were asked to recommend companies, I wrote people from my network, and companies named in the TU Delft monitor report are approached. There is a high risk of self-selection for the recruitment of hosting providers. Companies with a particular point of view or interest are probably more willing to participate. Also, companies named in the TU Delft reports could be unwilling to participate because of the topic's political sensitivity.

The hotlines are selected based on relevance to the Dutch CSAM NTD mechanism. Experts from INHOPE, industry representatives, the Dutch Police, the Ministry of J&V, and EOKM recommended recruiting the UK, Canadian, US, and France hotline.

Most participants are recruited based on existing relations. Some are recruited through the general contact information found online. Others were recruited based on the recommendation of other participants, a so-called snowballing effect.

Interview protocol and questions

The interview protocol consists of two main parts. First, providing information and asking permission regarding data gathering, storage, and use. Second, the main interview questions. All interviews included an interview opening and an interview closing, which can be found in the interview protocols in Appendix B. The first part is more thoroughly described in section 5.3.2. The interview questions aim to gather information on the three topics as defined in section 5.3. First, mapping the internal processes and the integral NTD mechanism and affiliated efforts. Secondly, revealing the position of stakeholders and how they participate in the policymaking process. Finally, creating an overview of how stakeholders evaluate the government policies and what kind of improvements they suggest to it.

The interview-questions are related to one of the components of the research sub-questions. The interview question is distinguished into four parts A, B, and C, and D. Part A aimed at unraveling the stakeholders' position, sub-question 2. Part B consists of detailed questions about the internal processes, sub-question 1. Part C asked to evaluate the current government policies and suggest improvements, sub-question 4 and 5. Lastly, part D aimed at mapping the participation of stakeholders in the policymaking process, sub-question 3. Part A, C, and D were centered around the perspectives and opinions of the participant. In contrast, in part B, an objective process description was asked. Part B, C, and D were designed per role and category of stakeholders. Part A, Part C, and Part D are based on the theory of the rounds model of Teisman (2000).

The semi-structured character of the interviews gave space to dig deeper during some interviews. Therefore, in every interview, slightly different questions are asked. In part A, questions were asked like: "what is your organization's mission concerning fighting CSAM?" and "Who do you believe is predominantly responsible for the functioning of the NTD mechanism?". These preliminary questions were for all stakeholders the same.

The questions in part B were asked according to the roles in chapter 4, in figure 5.3 the same figure can be found.

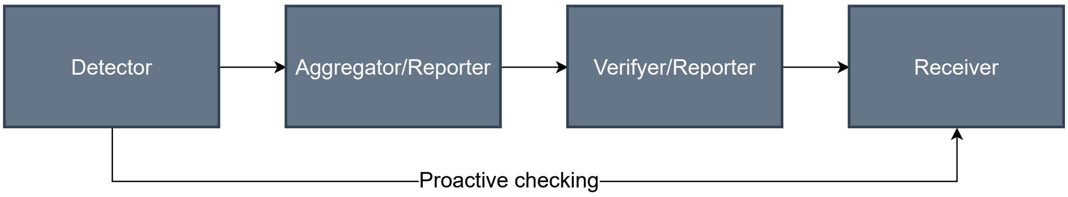

Figure 5.3: Repetition: CSAM NTD mechanism

Dependent on how the stakeholders defined their role during the interview, specific questions about their processes were asked. In table 5.3 a few example questions are given for the different specified roles. It is important to note that role of the "receiver" includes reactive and proactive processes. The organizations did not need to give the precise title of their role, but based on their description of the processes, roles are matched. Some participants did not have a specific role in the execution of the NTD mechanism and affiliated instruments. For those stakeholders, Part B was skipped.

The interview questions in part C were adapted to the stakeholders' role in the policymaking process, as shown in table 5.4. The participants were asked to evaluate the government policies in general. During the interviews, the participants were challenged to explain why they believed certain things and on which facts

Part B: Process descriptions - example interview questions				
Detector	Aggregator	Verifier	Notifier	Receiver
- What are the protocols for finding CSAM? - Which methods do you use?	- What are the protocols for aggregating reports? - From which sources do you receive reports?	- What are the protocols for checking CSAM reports? - What are your decision criteria on which report you are going to handle first?	- What are the protocols for notifying? - When do you sent a takedown request to a company?	- What are the protocols you have in place for taking down CSAM? - What are the protocols your organization has in place for a proactive NTD mechanism?

Table 5.3: Example Question - Part B: Process descriptions

they based them. In the second section of part C, more specific questions were asked about the warning letter the Ministry of Jsent in June 2020 and the published TU Delft monitor report in October 2020. PPC members were first asked about their policies' objectives and expectations. Then they were asked to reflect on their expectations in comparison with the real effect. The other stakeholders were asked how they evaluated these policies. The hosting providers were asked if they received a letter or were named in the TU Delft monitor and what kind of effect it had on their companies. Finally, the stakeholders were asked to suggest improvements to the government policies.

During part D, questions have been asked about the participation of stakeholders in the policymaking processes. All relevant policy arenas are considered: the PPC, the EC, INHOPE, RIPE NCC, and self-regulation. Specific questions are asked dependent on the international or national focus of the organizations and the institutions in which they are involved. Examples of specified questions and the used classification can be found in table 5.5. The Ministry of Jand the Ministry of EZK and EC have legislative roles. Traditionally, these organizations are decisive and take a central leadership role. Participation and joint policymaking are only possible if those organizations involve other stakeholders (Teisman and Klijn, 2002). Therefore, the legislative organizations are asked several more questions on how they involve other actors' processes. Also, their perspectives on participation are asked.

Qualitative interview data processing & analysis

In preparation for the qualitative data processing and analysis, all interviews were recorded and transcribed word for word. Qualitative data gathering often results in large quantities of data. Accordingly, the processing and analysis of qualitative data are split up into three stages. The three stages are (1) data reduction, (2) data displaying, and (3) concluding the data (Miles and Huberman, 2014). During the phases of data reduction, the interview reports are coded. Those codes are clustered and rearranged (Sekaran and Bougie, 2016). After the data reduction stage, the data is displayed. Data can be displayed in many ways. The goal with data displaying is the support the explanation of results by making it easier and more appealing to read. Data displaying can be done using quotations, tables, graphs, figures, and charts (Horton et al., 2004). This report used mostly tables and figures, specifically flow charts, for data displaying in chapter 6 and chapter 7. The last stage is concluding the data. In this study, there is a

Part C: Functioning of current policies and efforts - example interview questions			
Facilitators (without Industry representatives)	Hotlines + TBKK + others	Hosting providers	Industry representatives
Dutch: - Was the effect of the naming-and-shaming similar to what you expected/wanted? *European Commission*: - What do you think of the monitor as implemented in the Netherlands?	*Dutch Police + hotline*: - What changes did you notice after the letters were send? Was the effect of the letters similar to what you expected/wanted? Foreign: - Did you see any changes in found reports or take down time in the Netherlands form June (letters)	- Did you receive a letter of the ministry of Justice and Security in June? ->If yes: Did you changed your policy or took action after receiving the letter?	- What did you notice within the industry after the naming-and-shaming? - Do you believe it motivated hosting providers in changing?

Table 5.4: Example Question - Part C: Functioning of current policies and efforts

Part D: Policymaking & participation – example interview questions		
Policymakers	Hotlines + TBKK +others	Hosting providers
- On which parts of policies do you feel your organization has influence? (National and International) - How do you involve other stakeholders in the policy-making process you lead? - Are you satisfied with the influence you have in the policy-making process of countering CSAM on the internet? And why?	- On which parts of policies do you feel your organization has influence? (National and International) - Are you satisfied with the possibilities to participate and the influence you have in the policymaking process of countering CSAM on the internet? And why?	- How are you able to influence the policy adopted by the Dutch government and the European Commission? - Are you satisfied with the possibilities to participate and the influence you have in the policy-making process of countering CSAM on the internet? And why?

Table 5.5: Example Question - Part D: Policy making & participation

conclusion written about some parts of the qualitative analysis. However, the main conclusions are drawn based on qualitative and quantitative analysis. The three phases of qualitative data processing and analysis are not conducted in a linear timeline. It is an iterative process and goes back and forth. All phases are discussed hereafter.

Data reduction

Interview reporting

The interviews were recorded with an audio recorder and with the video-conference program Big Blue Button provided by TU Delft. Those interviews were transcribed word for word. Redundant and repeating information was left out of the transcription.

Coding

In general, in literature, four types of coding methods are distinguished: deductive, inductive, open, and selective (Emans, 2004). In this research, solely deductive coding on a categorical level is applied. Before the coding and establishment of the interview protocols, this study's relevant themes were already established. The interview questions are intended to reveal information about the different categories. Paragraphs and sometimes lines were coded with a category. Because of the categorical level, no new insights are excluded due to too pierced coding. Therefore, it was appropriate to use deductive coding (Creswell and Tashakkori, 2007). This research aims to reveal the difference and relations between stakeholders. Some codes are therefore specified per actor group. In total, 12 categorical codes, the codes including descriptions are displayed in table 5.6

Overview codes	
Category	*Description*
Characteristics organization	Descriptive on purpose, coordinated effort, division of labor
Objective – Mission	The mission of the organization regarding fighting CSAM
Motivation	The incentive to take action regarding CSAM
Responsibility	Who should be responsible for which part of the policies according to the interviewee
Role	Which role the organization believes to have in the government policies
Process descriptions	The detailed internal process descriptions of the procedures around CSAM
General abuse handling (only hosting providers)	How internal general abuse handling stands in relation to CSAM handling
Evaluation of the current policies: -General -Naming-and-Shaming	The perspective of the organization on the adequacy and effectiveness of the government policies
Challenges/Risks of CSAM	Which challenges and risks are affiliated with the fight against CSAM
Improvements	Which improvements the organization believe to be most effective
Financing	Who should be responsible for financing which part of the policies according to the participant
Participation: -NL -Self-regulation -EU -INHOPE -Ripe NCC community	The satisfaction and effort concerning the policymaking process. This also includes the (in)formal relations between actors

Table 5.6: Codes and descriptions

After the interviews' coding, a distinction is made between the process descriptions and the results affiliated with the rounds model. The process descriptions are summarized per stakeholder. It is decided to show summaries instead of quoted interviews because of the high volume of data, anonymity, and political sensitivity. Furthermore, including the interview transcripts would provide the reader with an excess amount of data, which cannot be overseen. Secondly, when having insights into the quoted interviews, it would be possible for certain people to recognize the interviewee. Lastly, recited interviews are not presented because some parts are politically sensitive and can cause conflict between the participants, while the statements are irrelevant to this study's conclusion. Moreover, most interviews were conducted in Dutch. For the summary, they are translated into English (VS) and omitted as little as possible. The participants approved the presented summaries.

Data display

Although the number of 12 different codes is not much, the coded information was enormous. All 21 interviews consisted of 15 to 24 pages. To provide readers with a coherent overview of the results, an appropriate discussion and form of data displaying is crucial. Predominantly, tables and flow charts are selected to present the results in an understandable matter. Some quotes are used to clarify the meaning of the participants.

Drawing conclusions and inserting insights into research report

After the summaries per stakeholder group, the data of the process descriptions are compared and analyzed. The rest of the qualitative data is analyzed to determine stakeholders' position, show how they participate in the policymaking process, evaluate the government policies, and suggest improvements to the policies. Also, the differences within the stakeholder groups are addressed.

5.3.1 *Merging and Analyzing of Quantitative and Qualitative Results*

The results of the quantitative and qualitative analysis are combined to answer the sub-questions. The findings of the qualitative analysis are weighted based on the quantitative analysis. The other way around the qualitative analysis can explain some parts of the quantitative analysis. Using both methods give a good overview of the relevance and the reason behind particular findings.

5.3.2 *Data management & Research ethics*

Before starting the interviews, the Human Research Ethics Committee of TU Delft approved the research. All participants were asked to sign an informed consent form before the interview. A non-singed example can be found in Appendix B. Those participants who did not return the informed consent form before the interview were asked to read it and consent during the interview. Consequently, some informed consent forms are audio-recordings. After receiving consent, the interviews were conducted online using Big Blue Button provided by TU Delft. All interviews were recorded with an audio-recording and with the program Big Blue Button. The audio recording was saved on a storage space SurfDrive provided by TU Delft and the recordings of Big Blue Button on a server of surf cloud. Before conducting the interviews, an appointment with the Data officer took place. All further data used is stored on SurfDrive. For processing and analyzing the qualitative data, the programs: word and Atlas.it is used. The quantitative data analysis is done with Jupiter Notebook and excel. The report is written in Overleaf. After the interviews were transcribed, all recordings were deleted. Also, there is no personal data stored from the participants. In line with that, the interviews are made anonymous. All stakeholders got the chance to withdraw at any given time during the interview and assess the report's information.

6
Results 1: Overview of the Mechanism

In the following two chapters, the results from both the quantitative and the qualitative analyses are presented. The sub-questions are answered in the following two chapters. Section 6.1 discusses the results of the quantitative analysis. For the quantitative results, the data of EOKM, the Canadian hotline, the UK hotline, and INHOPE is analyzed. The qualitative results are based on 21 conducted interviews with 19 different organizations. Table 5.2 states an overview of the interviewed stakeholders. The interviews are conducted in October and November 2020. Due to the COVID-19 pandemic, all interviews were conducted online. The interview duration was 47 to 89 minutes, with an average of 71 minutes.

This chapter answers the first sub-question.

Sub-question 1

How does the Dutch NTD mechanism and the HashCheckService look like in terms of processes, information flows, and processing times per organization?

Section 6.1 discusses the finding from the data analyses and reflects on the results of the Canadian hotline's data regarding the TU Delft monitor report. In section 6.2, the internal processes of organizations participating in the NTD mechanism are stated. Those Internal processes of similar stakeholders are compared. In chapter 7, sub-question 2, 3, 4, and 5 are answered. In section 7.1 the positions of the stakeholders in the policy-arena are considered and in section 7.2 how the stakeholders participate in the policymaking process. Section 7.3 presents the evaluation of the stakeholders of the government policies following the four policy lines. In section 7.4 the quantitative and qualitative analyses are combined. The combined outcomes are used to select and discuss proposed improvements to the government policies. Stakeholders suggest improvements to the government policies during the interviews.

6.1 Quantitative overview of the NTD mechanism and the HashCheckService

In this section, the information flows of the Dutch NTD mechanism and the HCS are mapped and quantified. Figure 6.1 displays a high-level flow diagram of the most relevant streams of reports to the Netherlands.

Figure 6.1 displays a high-level flow diagram of the most relevant streams of reports to the Netherlands.

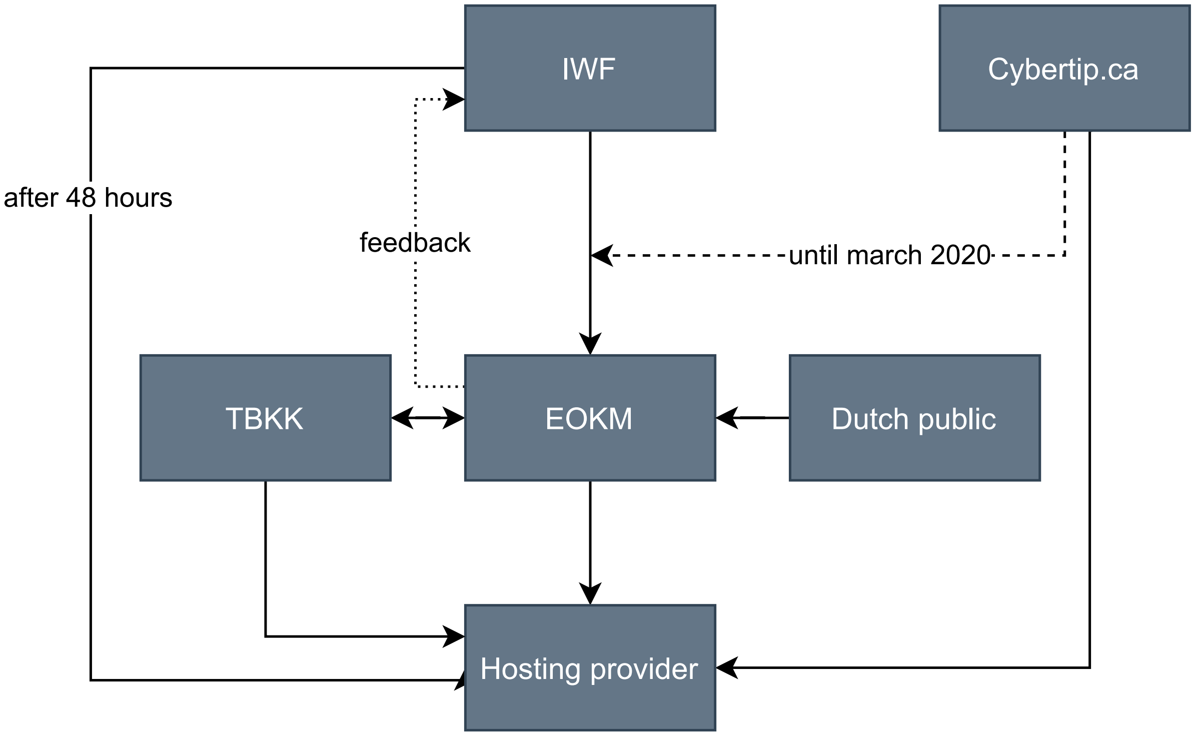

Figure 6.1: Overview of the Dutch NTD reporting mechanism

The results are discussed in order of the Dutch NTD mechanism. Starting at the incoming reports to the Netherlands, processing of reports by EOKM, sent takedown requests to Dutch hosting providers. Then the distribution of CSAM on the Intentioned and the takedown time of Dutch hosting providers are addressed. Lastly, the number of reports found by the HCS are discussed. When relevant, possible effects of the warning letters (Policy 1, June 2020) and polishing the TU Delft monitor report (Policy 2, October 2020) are considered.

6.1.1 *Received reports*

EOKM receives reports from three sources: 1. INHOPE, 2. The Dutch Public, 3. The Dutch Police. For the latter, EOKM does not track data. Reports that EOKM receives are categorized as illegal or not illegal and hosted in the Netherlands or hosted abroad.

In 2018 and 2019, 76% of all illegal and non-duplicate reports EOKM received originated from INHOPE members. The other 24% is obtained from the Dutch public and displayed in figure 6.2. Accordingly, EOKM is predominantly dependent on foreign hotlines for the largest share of its received reports.

According to INHOPE, the Canadian and UK hotline provided by far the most significant share of reports to the Netherlands the past three years, shown in figure 6.3. The UK hotline reported 23% in 2018 and 19% in 2019 of all INHOPE reports to the Netherlands. The Canadian hotline was responsible for respectively 72% and 76%. As the Canadian hotline left INHOPE in March 2020, INHOPE has no clear picture of

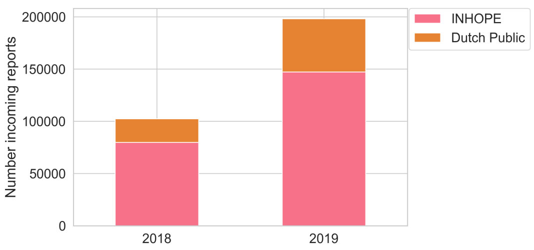

Figure 6.2: Distribution of source of incoming reports EOKM 2018 and 2019

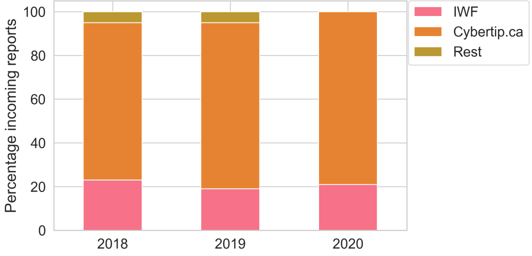

Figure 6.3: Distribution incoming reports EOKM INHOPE

Canada's reports sent to the Netherlands. Preliminary data of the Canadian hotline and the UK hotline indicate that the distribution of both hotlines' contribution in 2020 is similar to that of the past years.

Remarkable is that according to (EOKM, 2020), the UK hotline accounted for 61,6% and the Canadian hotline for 23% of the illegal notification from INHOPE in 2019. A different distribution is found in the data delivered by INHOPE the Canadian and UK hotline. They report the total amount of reports the other way around, namely 76% for the Canadian hotline and 25% for the UK hotline. This difference could be explained by the fact that EOKM reports unique and illegal reports. Accordingly, EOKM excludes all URLs that are reported multiple times. The data sets' differences could be explained by an abundance of duplicates in the URL's the Canadian hotline reported. However, this is unknown.

6.1.2 *Processing time EOKM*

When the EOKM classifies reports as illegal and hosted in the Netherlands, a takedown request is sent to the corresponding hosting provider. The time between receiving and sending a takedown request is called the processing time. The analyzed data only includes URL's that are hosted in the Netherlands. EOKM processed a total of 23994 reports between the 23rd of October and the 21ste of December 2020. During the last days of October, EOKM sent 3417 takedown requests. The EOKM sent 6950 in November and 13627 in December. Notable is the difference between November and December. At the end of the period, 703 reports were not processed. Some of those non-processed reports were received over a year ago. Figure 6.4 displays the processing time of EOKM per hour and category. The graphs show that 53% of the reports (12850) are processed immediately without delay. Within 24 hours, 88% (21239) reports are processed. When the 703 not processed reports are included in the data, not 88% but 86% (21944) of the reports are processed within 24 hours. After 48 hours, 11,4% (2825) is not yet processed, and after 72 hours, 7% (1734) is still not processed. The lower right graph displays the processing time for reports not processed within 48 hours. Most of the reports are processed between 48 hours and 150 hours and some after 2000 or even 7000 hours.

6.1.3 *Sending takedown requests*

Figure 6.5shows that the sent takedown requests per month highly fluctuate. The data shows no clear relation between the two policy events (warning letters and publishing the TU Delft Monitor report) and a change in the number of sent takedown requests. The period after the first policy (warning letters) is from "June-Oct 2020". The second policy (publishing the TU Delft monitor report) period is "from October 2020".

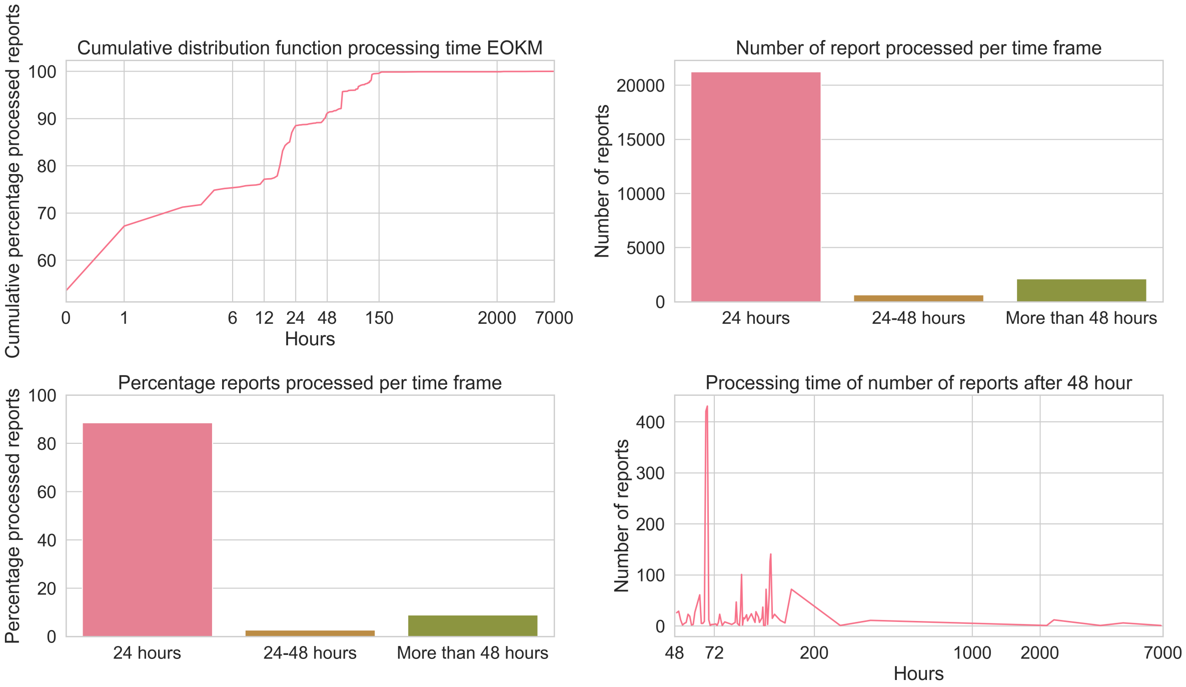

Figure 6.4: Processing time EOKM from reports processed between 23rd of October and the 21st of December 2020

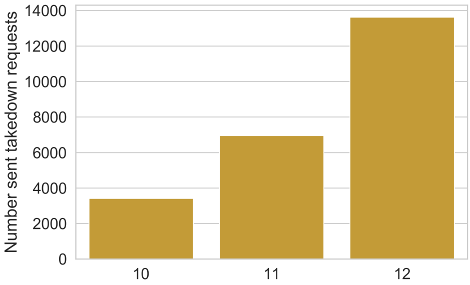

Figure 6.5: Number of sent takedown requests per Month - 23 October - 21st of December 2020

6.1.4 *Distribution of CSAM*

The Canadian hotline data showed that significantly fewer takedown requests for unique reports are sent in 2020 than in 2019. Also, is the distribution of which hosting providers host CSAM different from what TU Delft found. The TU Delft monitor report shows that one hosting provider is 2019 responsible for 72.3% of all hosted CSAM. Taken from Jan - Aug this is even 93% of all the uniquely reported CSAM (Lone et al., 2020). This distribution is not observed in the data of the Canadian hotline. Figure 6.7 shows that in 2020 Company 1 is responsible for between 25% and 60% of all reports, but it is highly fluctuating. The top 5 companies account for between 80% and 53% percent of the total reports. Significantly less than in the TU Delft report. That implicates that the variance of companies that host a lot of CSAM is more considerable for the Canadian data. Furthermore, figure 6.6 shows that the Canadian hotline sent fewer

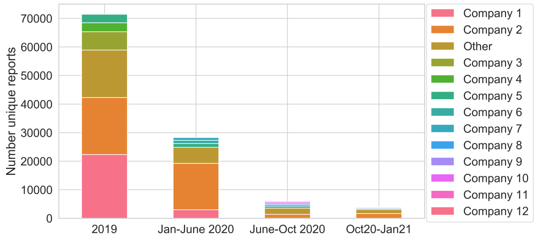

Figure 6.6: Top 5 hosting providers

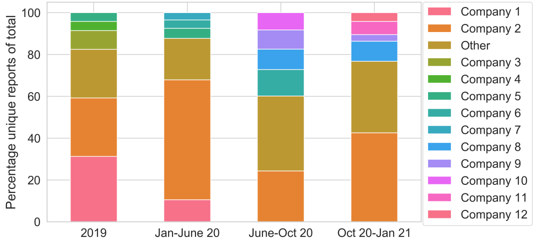

Figure 6.7: % URLs per hoster per month 2019/2020

takedown requests in 2019 than in 2020. The Canadian hotline noted that in 2019 they directly targeted "chan" sites hosted in the Netherlands caused a significant increase in the reported CSAM.

The Canadian data also shows similarities to the findings of the TU Delft monitor. The top 5 companies of 2019 and 2020 of the Canadian hotline data are partly similar to the companies found by TU Delft. Five of the eleven Canadian identified companies are also found by TU Delft in the reports of 2018, 2019, and 2020. However, their place in the ranking is different in both findings. The Canadian data is included in the data used by TU Delft for the monitor until 2019. The difference in the top fives of the Canadian hotline data and the TU Delft monitor in 2019 could reflect that different hotlines find CSAM in various distributions and at other companies. The top five of the TU Delft is not a perfect reflection of all separate hotlines. Accordingly, some hotlines can find many reports of one company and another hotline of another company.

6.1.5 *Takedown time of Hosting Providers*

The takedown time is measured from the moment the Canadian hotline sends a takedown request to the hotline's last date to send a takedown request. Figure 6.8 shows how many reports are taken down within 24, between 24-48, and after 48 hours for each month. It displays that less CSAM was reported to companies in absolute numbers in 2020, and less material remained online for longer than 24 hours. The policies indicated per time period in figure 6.10, do not indicate an evident change in reports. When looking at figure 6.10, it seems that there is a little increase of material taken down within 24 hours after the first (June 2020) and second policy (Oct 2020). The Canadian data shows that in 2020 from January to June, just 52% of the material was deleted with 24 hours. From June to October, this was 55%, and from October 2020 to January 2021, it was 75%. But the TU Delft monitor reported that companies took 84% of the material down within 24 hours. The Canadian taken down reports within 24 hours are therefore significantly different than what TU Delft has found.

Furthermore, figure 6.11 shows a boxplot of the takedown hours' distribution per period. The boxplot takedown hours' variance reduces per period, implying that more reports are deleted within shorter time frames. Furthermore, the outliers of takedown hours become smaller in duration. However, a maximum value does not necessarily mean the report is actually taken down. The shorter tails may be a direct result of the time frame of the data set.

Figure 6.12 displays per company how many percent of the received reports are taken down within 24 hours (x-axes), between 24 and 48 hours (darkness of the color), or after 48 hours (y-axes). The size of the bubbles indicates the total amount of takedown requests that each company received. All graphs seem to

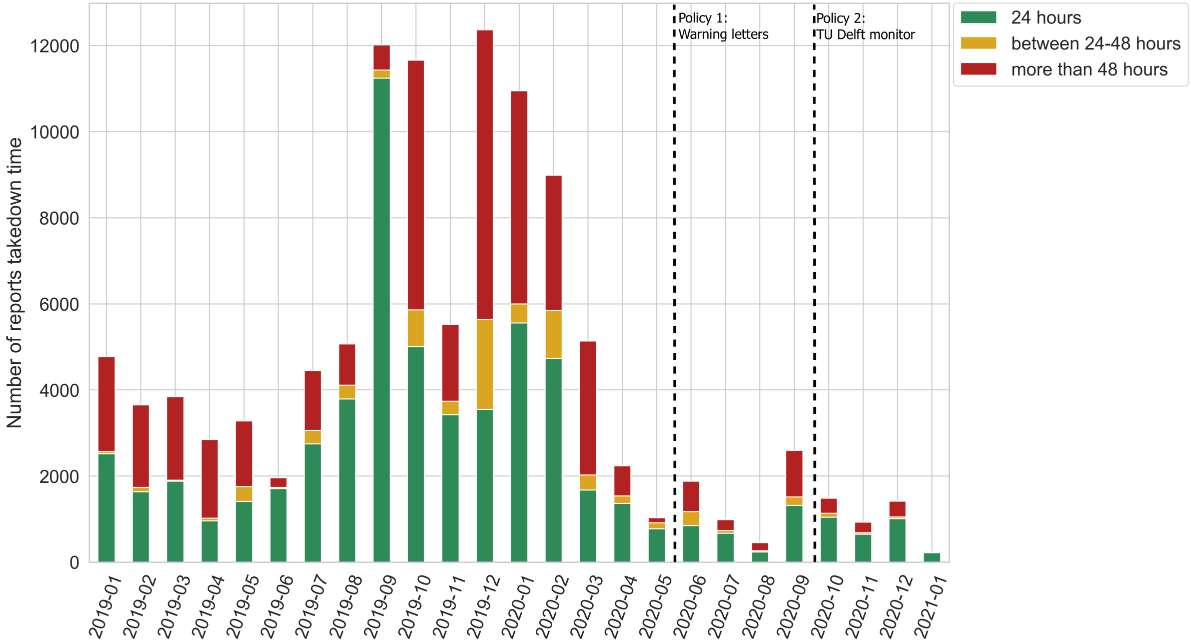

Figure 6.8: Take down times measured by the Canadian hotline 2019, 2020, 2021

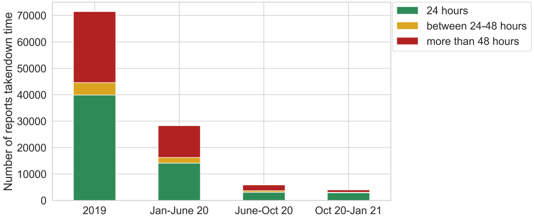

Figure 6.9: Takedown time total

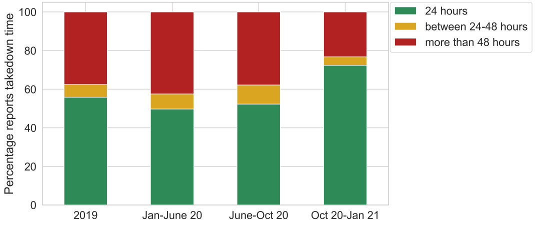

Figure 6.10: % Takedown time

show a diagonal line from 100% taken down within 24 hours on the x-axes to 100% taken down after 48 hours on the Y-axes. That means that companies predominantly take down material either within 24 hours or after 48 hours. Accordingly, not many companies are often just missing the 24 hours norm. Further, it seems that over time and after the two policies (June 2020 and October 2020), more companies deleted a higher percentage of takedown requests within 24 hours, this is displayed in the two lower graphs. The graphs also show that companies' performance is quite diverse. It seems that over time companies choose a side, deleting content within 24 hours or after.

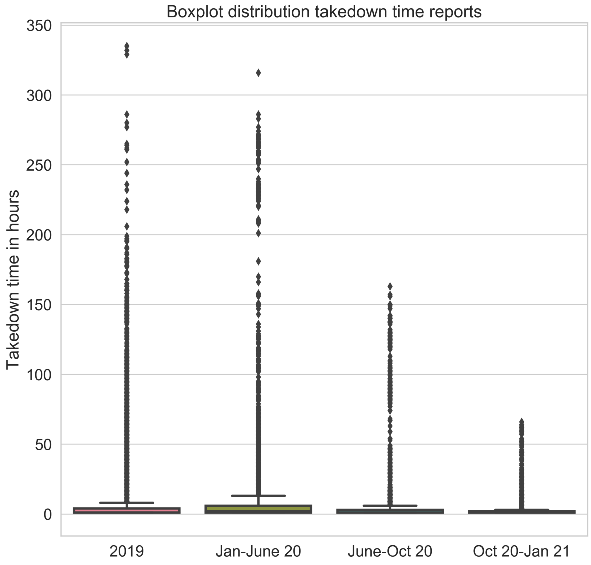

Figure 6.11: Takedown time distribution total hours

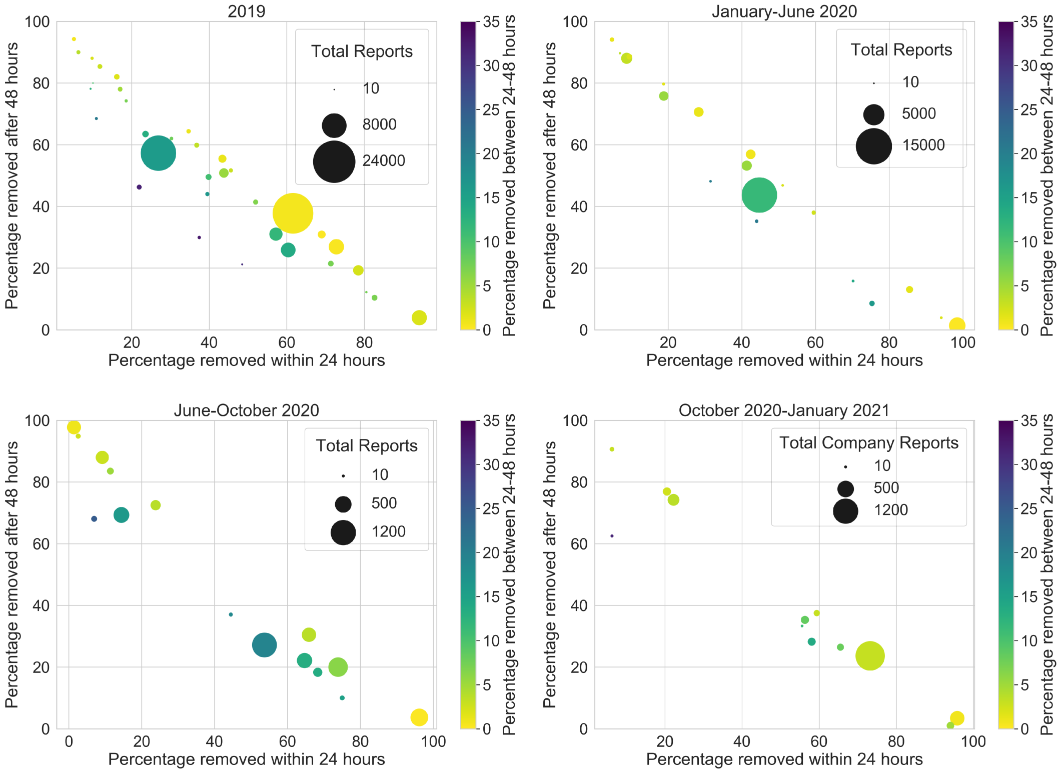

Figure 6.12: Takedown time distribution Companies

6.1.6 *HashCheckService*

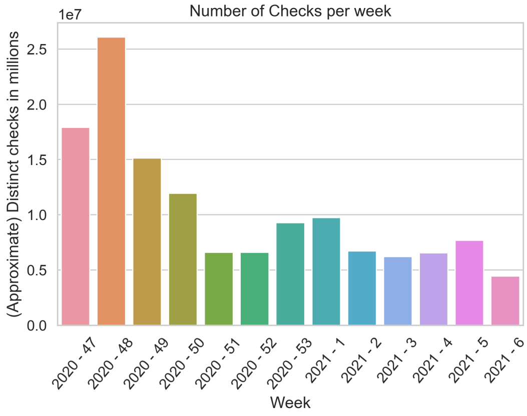

Figure 6.13: HCS checks November 2020 - Febraury 2021

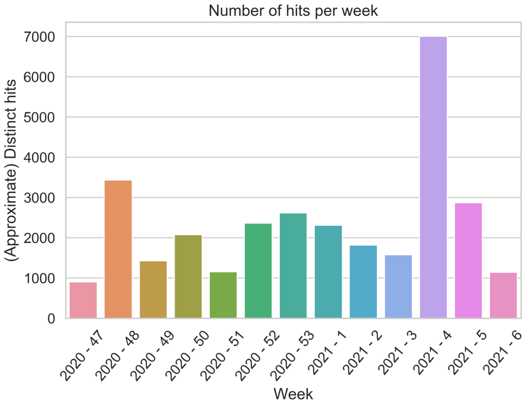

Figure 6.14: HCS hits November 2020 - Febraury 2021

The number of checks and hits of the HCS from week 47 2020 to week 6 2021 shows significantly less found material than the results of the HCS until week 39 2020. Until week 39, the HCS already got more than 7 million hits. A hit is a match with the checked content and the hash database (**?**). While from week 47 2020 to week 6 2021, the number of hits seems steady between 1000 and 3000 every week. Week 4 of 2021 was an exception as around the HCS reported 7000 hits. Even if every week just 1500 reports would be detected with the HCS, at the end of the year, around 80.000 reports are directly notified, which is one-third of the reports EOKM processed in 2019 (EOKM, 2020).

EOKM noted that the decrease of the hits and checks is expected as in the first weeks, the plugged-in companies checked there all the content on their servers from even years old, and now they keep up with newly uploaded material. Furthermore, it is essential to note that the material is differently reported now. The results of 2020 until week 39 included also duplicate checked reports (Grapperhaus, 2020a). Now only the unique matches per week are displayed. If, after a week, companies still did not take the material down, the HCS gives a hit again.

Currently, around 54 companies are plugged into the HCS. Most of these companies started using the HCS after the Ministry of J&V send the warning letters in June. Some of them were already active before the warning letters, and some became active after the TU Delft monitor report was published.

6.2 Processes hosting providers, hotlines, TBKK and INHOPE

In the following sections, the processes of organizations in the CSAM NTD mechanism are described and compared. First, the detecting aggregating, verifying, and reporting processes of the hotlines are set-out and compared. Additionally, the activities around their role within the NTD mechanism, such as monitoring and proactive searching, are described. Secondly, INHOPE's process is outlined. Thirdly, the NTD and affiliated processes of the hosting providers are described and compared. Lastly, the process of TBKK is mapped.

6.2.1 *Hotline processes*

The role of the hotline in the Dutch NTD mechanism is diverse. Within the Dutch NTD Mechanism, the hotlines find, aggregate, check and report CSAM. Figure 6.15 displays the process of EOKM. Table 6.1 displays the characteristics of the hotlines.

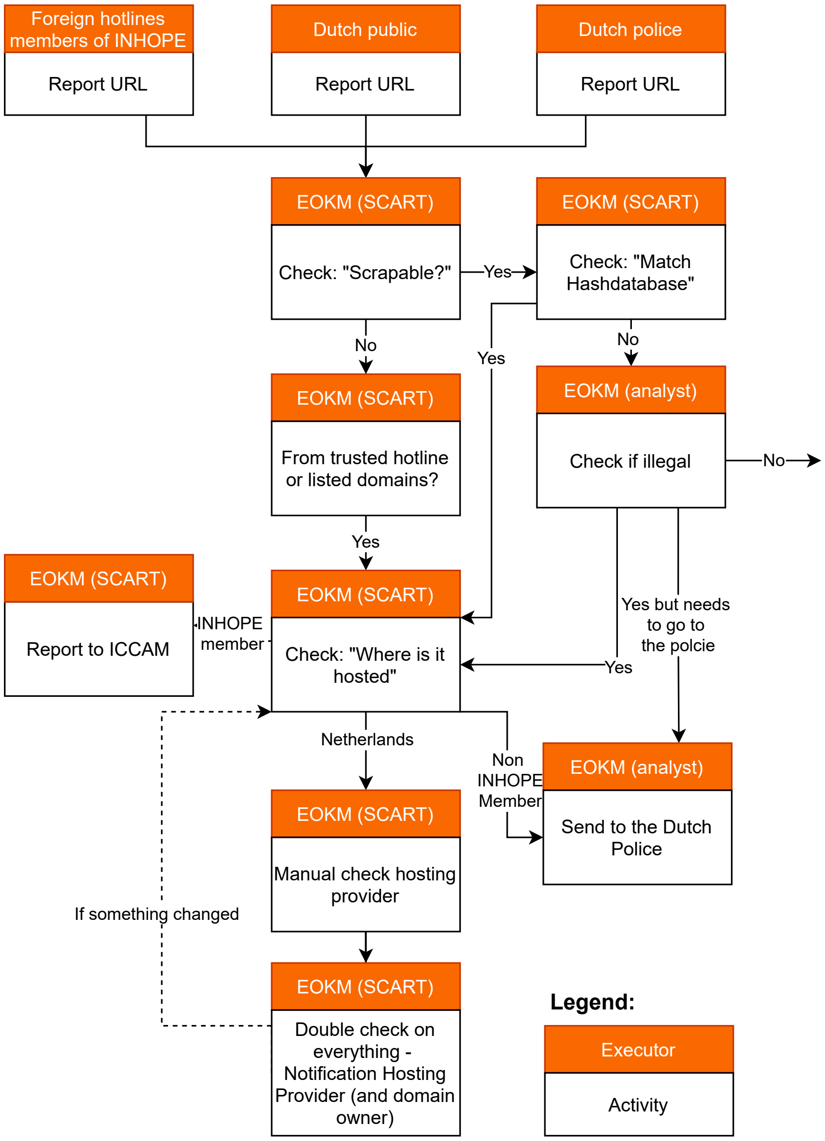

Figure 6.15: Internal processes EOKM

	HL NL	HL UK	HL Canada	HL France	HL US
Analyst FTE	9 analysts	13 Analyst, 20 work with content	10-12 analyst	3 analysts	Up to 35
Member of INHOPE	Yes	Yes	No	Yes	Yes
Main source of inflow of reports	INHOPE	Proactive search	Proactive search	Public	Industry
Main source of financial resources	Public institutions & industry	Industry	Public institutions	Public institutions & industry	Government & industry
Roles	Aggregator, Verifier, Notifier	Detector, Aggregator, Verifier, Notifier	Finder, Aggregator, Verifier, Notifier	Aggregator, Verifier, Notifier	Aggregator, Verifier, Notifier
Focus point	CSAM	CSAM and missing children	CSAM and missing children	CSAM and Terrorist content	CSAM and missing children
Backlog	Sometime, (decreasing)	No	Yes	No	Not really

Table 6.1: Hotline characteristics as defined by themselves

Finding

EOKM receives reports from three sources: INHOPE, the Dutch public (through e-mail and their web form), and the Dutch Police. The reports through INHOPE are provided by foreign hotlines. Within those hotlines, the reports also come from different sources. All interviewed hotlines receive reports from the national public through Internet forms, apps, telephone hotlines or like the French hotline through a mobile app. The UK and the Canadian hotline do not only receive reports from the public but also search proactively for material online. The US hotline receives reports from companies due to the mandatory reporting requirements present in the US. Here it is important to note that reports made through a mandatory reporting requirement are already taken down.

Proactive searching and WebCrawler
It depends on country regulations if proactive searching and web crawling is allowed. The Canadian and the UK hotline are both allowed to search proactively with a web crawler. The US and the France hotlines are not allowed to crawl the Internet. But they are allowed to click through from a reported URL. EOKM is not allowed to do any of these actions.

The Canadian and the UK hotline proactively and automatically crawl the Internet. The UK hotline operates a web crawler, which functions as a spider. The spider works as follows: it starts manually somewhere on the web. A UK analyst sets the manual location. This starting position is always a place on the Internet with an already known high risk of finding CSAM. A high-risk area of CSAM can be a reported URL with CSAM or domains/webpages where CSAM is often found. Based on predefined words or other indicators, the spider goes through hyperlinks on the webpages. The spider scrapes images from the Internet and checks if they are CSAM. To be able to do this, the spider is linked with a hash database and uses PhotoDNA. How far and how long a spider will crawl can be customized by the analysts using it. The UK hotline chooses explicitly to use the crawler in a targeted manner. That means that they usually let the spider start at a position in which they are assured to come across a high ratio of CSAM. Also, the accuracy of PhotoDNA is set high to prevent having too many non CSAM pictures. The targeted usage and the high setting of the PhotoDNA accuracy level match the available analyst's capacity to avoid a backlog. If the crawler has found CSAM, there is always a manual check by a UK analyst to prevent false positives.

In essence, the Canadian WebCrawler works the same as the UK crawler. However, the Canadian hotline uses it in two ways. Firstly, similar to the UK, the crawler is assigned a starting point at a known URL, domain, or public report. From there, it will click through links that are mentioned on the webpages. The other method is to use the WebCrawler to search on the dark web. The web crawler will go through hyperlinks shared on the dark web fora to the open web. All images are compared to their hash database with the use of PhotoDNA. If it is a 100% match, no further manual assessment is done. If the match is less than 100%, they have a tiered classification system. If it almost 100%, just one analyst is asked to check the image. If the match is not very reliable, up to 3 analysts are asked to assess the content. The classification is not only done by the analyst of the Canadian hotline. Eight other hotlines joined their web crawler classification. The Canadian hotline has chosen to lower the accuracy of PhotoDNA, compared to the UK hotline, to find more illegal material.

Aggregating and Verifying

Reports are URL's with content that is potentially CSAM. EOKM receives reports from three sources: INHOPE, the Dutch public, and the Dutch Police. The reports from INHOPE and the webform are automatically extracted by SCART. SCART saves all reports and puts them in a queue to process. First, SCART looks if an URL is reported by a reliable INHOPE hotline and if the image is hosted on a green listed domain. EOKM has a green list of companies that they believe are trustworthy, cooperative, and receive reports regularly. If the report is sent by a reliable hotline and hosted on a green listed domain, SCART does not scrape the image and immediately classifies it as illegal. If not, then SCART tries to scrape the content, creates a hash, and tries to classify it by comparing the hash to the hashes in the Hashdatabase of EOKM provide by the Dutch Police. Since the end of January 2021, EOKM also uses photo DNA to classify content. If SCART cannot scrape an image, for example, because it is protected by a CAPTCHAS or references or the hash is not included in the Hashdatabase, an analyst will manually access and classify images. Furthermore, it has to be noted that analyst can only classify matertail up to 4 hours a day because of the mental strain affiliated with watching this content.

The difference with foreign hotlines compared to the EOKM
The aggregating and classifying processes of the foreign hotlines are comparable to the processes of EOKM. They only use different automatic systems. Interestingly, the Canadian hotline also has a technique that can also scrape most images behind CAPTCHAS and References. The systems and databases used to classify the content are also different. Most hotlines use PhotoDNA to compare the content with already known content. EOKM start doing using PhotoDNA in January 2021. Further, are the Hashdatabases different. In all databases, Interpol's ICSE database is included, and local law enforcement data can be different in every country. Moreover, the Canadian hotline maintains its own database and includes self-classified images without law enforcement involvement. EOKM, the US, and France hotlines seem to have relatively less automatized systems than the UK and Canada.

Reporting

If an image is classified as illegal, SCART will add the hosting information based on the WHOIS Ripe database. An analyst always double-checks this information. If an URL is hosted abroad in a country with a member of INHOPE, the URL is reported to INHOPE. If the report is hosted abroad, but if there is no hotline or the hotline is not a member of INHOPE, EOKM reports the URL to the Dutch police. The Dutch policy then reports it to the national police of that country. When the material is hosted in the Netherlands, the content is classified illegal. And if the hosting information is correct, a takedown request is sent to the hosting provider through SCART. If the domain owner's abuse contact information is known, EOKM also sends the hoster a takedown request.

There are a few exceptions. Firstly, when EOKM believes a law enforcement agency should assess the content, they do not send a takedown request but forward the report immediately to the police. Secondly, in some specific cases, EOKM sends a takedown order to the hosting provider and simultaneously to the Dutch police.

Foreign hotlines
Most hotline processes for sending takedown requests are quite similar to that of EOKM. Different are the processes applied by the Canadian hotline. Since the Canadian hotline is not a member of INHOPE anymore, their content-hosted abroad procedure is divergent from other hotlines. When a report is hosted outside Canada's jurisdictional boards, the Canadian hotline sends a takedown request directly to the hosting provider and skips the foreign hotline and INHOPE.

Furthermore, there are differences in the notification process. The UK hotline always needs to check with law enforcement before sending a takedown request. The France hotline needs to send all URLs to law enforcement if it is illegal but does not ask them for permission before issuing a takedown request. The US hotline has a similar agreement as the Netherlands. They do not have to ask permission and only send a report if they believe it is crucial for Law enforcement. Furthermore, the US hotline also sends international reports directly to the hosting providers if they are in close contact with them.

Monitoring and Escalating

After EOKM sends a takedown request to a hosting provider, they monitor if the content is taken down. If the image can be scraped by SCART, the image will be checked automatically every 4 hours. If the image cannot be scraped by SCART, an analyst of EOKM checks manually if the content is taken down. EOKM strives to checks all images at least every 24 hours. Both the automatic and manual checks are saved in SCART. If the image is still online after 24 hours, a reminder to the hosting provider is send. The procedures of EOKM dictates that when content is still online after 120 hours (4 takedown request), EOKM will send the fourth reminder to the hosting provider and simultaneously a request to the top domain registrar of the used domain. EOKM requests the top domain register to take down the domain or specific web page. Although EOKM strives to follow this procedure, this is seldom put into practice due to capacity limitations at EOKM. Figure 6.16 below shows the process of monitoring and further actions.

Foreign hotlines
Compared to other hotlines, the procedures around monitoring and escalating are very different. Firstly, the time limit in which hosting providers are expected to take down material is different per hotline. The Canadian hotline, analogous to EOKM, sends reminders every 24 hours. The US hotline applies a time limit of 72 hours. The French and UK hotline comply with the formulation in their national law "as soon as possible". In practice, that means that the time limit is flexible. The UK hotline has a proactive approach

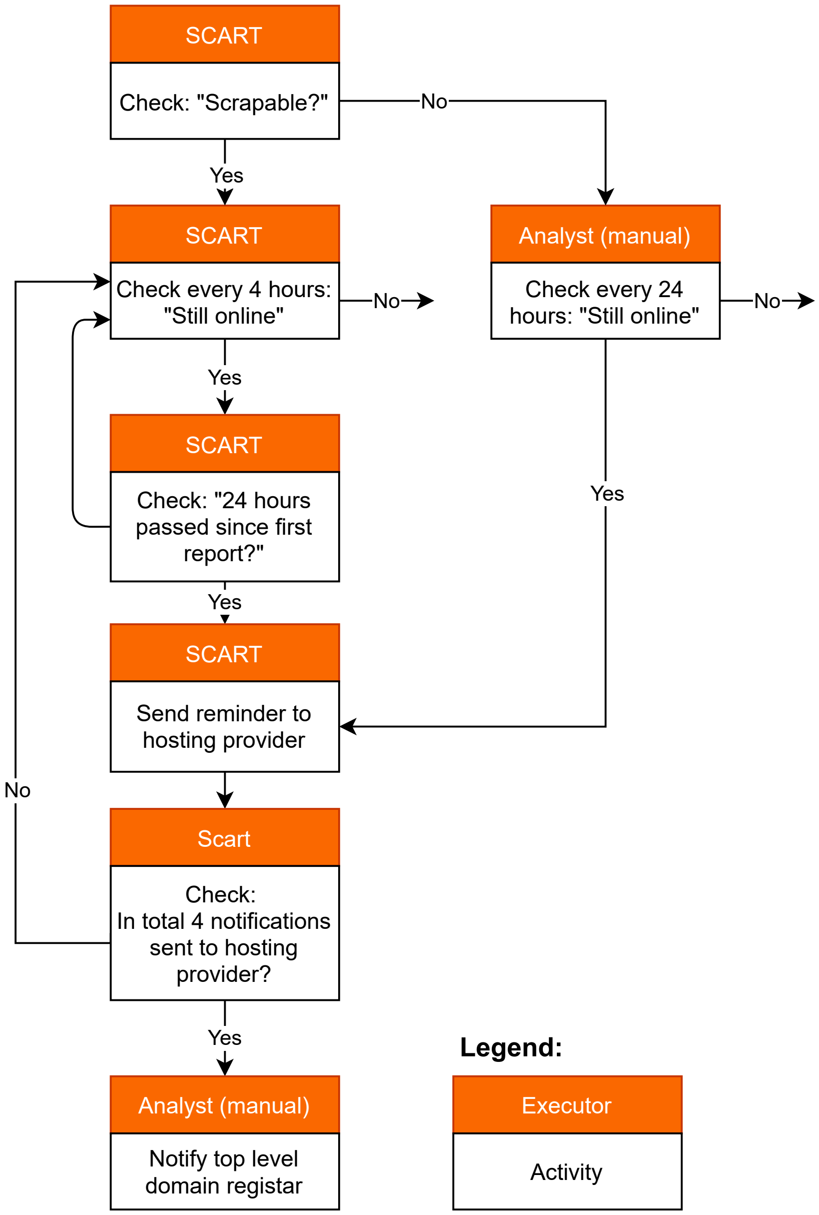
SCART
Check: "Scrapable?"
No
Yes
SCART
Check every 4 hours: "Still online"
No
Analyst (manual)
Check every 24 hours: "Still online"
No
Yes
SCART
Check: "24 hours passed since first report?"
Yes
Yes
SCART
Send reminder to hosting provider
No
Scart
Check: In total 4 notifications sent to hosting provider?
Yes
Analyst (manual)
Notify top level domain registar
Legend:
Executor
Activity

Figure 6.16: Internal processes EOKM Monitoring

to this. If the UK hotline has the hosting provider's telephone number, it follows up takedown requests with a phone call. The hotline will perform many follow-ups over the phone and e-mail if a hosting provider does not take the material down soon enough. Sometimes even several calls a day are being made. The time limit is therefore often shorter than 24 hours. The French hotline determines the time limit "as soon as possible" per hosting provider based on the specific circumstances. Accordingly, the takedown time can be hours or days. The US, Canadian, UK, and French hotline will also get law enforcement involved if companies take too long to takedown material. When exactly it takes too long is not defined.

Furthermore, the UK hotline does not only monitor and remind hosting providers but also monitors reports send to foreign hotlines. The UK hotline monitors the URLs they sent through ICCAM. If, after 24 hours, the URL is not taken down, the UK hotline sent a reminder to the hotline. If, after 48 hours, the URL is still online, the UK hotline will send a notification directly to the hosting provider. Although sending a reminder complies with the INHOPE rules, the UK hotline is from the interviewed hotlines, the only one that is doing this.

Affiliated instruments and activities

Next to the reactive activities, which fit into the NTD mechanism, hotlines also offer preventive and other affiliated activities. All hotlines send takedown requests for free. Almost all hotlines also offer preventive and other affiliated instruments for free, except the UK hotline. The UK hotline offers memberships to companies and provides services to its members. The Canadian and US hotline services can be used by all companies around the world free of charge. For now, Dutch companies can only use the services of EOKM.

Preventive filters HashCheckService All hotlines, except the French hotline, offer some preventive filters for the industry. EOKM offers the HashCheckService, which is a service offered by EOKM to domains. Domains can plug into the system and compare the hashes from the content they host with the hashes in the database. Hosting providers cannot plug into the database but can ask their clients to plug-in to the HCS or again ask their clients to plug-in to the HCS. In general, there are two ways domain owners can use the HCS. They can scan their services at any given time or check newly uploaded pictures. The latter comes close to an upload filter, but it is not an filter because content is already uploaded onto the server. Furthermore, it is important to note that the HashCheckService only reports matches to the user but cannot automatically delete content. The HashCheckService is based on the HashDatabase of EOKM. EOKM is also developing a feature of the HCS that shows if the same URL is repeatedly reported.

The Canadian, US, and UK hotlines also offer hash services to companies which companies can use to proactively scan or preventively filter their services. The US hotline offers three kinds of platforms: (1) a hash database of CSAM with 6 million entries provided by NCMEC and two other non-governmental organizations, (2) a database linked to a platform on which industry members can exchange hashes with each other. NCMEC monitors all entries added by the industry members and complement the database, (3) a hash database provided and maintained by NCMEC with material on which children victims are exploited, including CSAM. The three platforms of the US hotline are only databases. Companies wanting to use one of the three can only retrieve the hashes but need to arrange a system themselves to scan or filter their services. Companies can, similarly to the HCS of EOKM, choose how to use the hashing lists. Some companies also scan private messaging applications on their platforms with the hashing lists of US.

Other instruments The UK hotline also provides a URL blocking list which consist of URL's on which CSAM is hosted. Telecom providers and other Internet access providers in the UK and worldwide will block the URL for its customers. Their customers are not able to visit the blocked URL's. This list is updated twice a day.

Connection to the Industry
EOKM has close contact with a few hosting providers in the sector. EOKM reaches out to a hosting provider who regularly receive CSAM. Together with the hosters, they try to improve the hoster's processes. The different hotlines have divergent ways how they relate to the industry. The UK and French hotline have close contact with the industry. Both hotlines also adapt their services to specific members of the

industry. The UK hotline keeps a very personal contact with the industry. The UK hotline works with memberships, and members pay between 1000 and 80.000 pounds per year. According to the UK hotline, they bridge the gap between policymakers/legislators and the industry. Industry members find a platform with a hotline to tell their perspective. The French hotline believes they are a bridge between the big platforms, the hosting sector, citizens, and the French authorities. One industry member takes place on the board of the French hotline.

In both models, the hotline is closer to the Industry than EOKM in the Netherlands. The US hotline relation with the industry is quite similar to the relationship EOKM has with the industry. They keep close contact, but the contact is mainly focused on improving processes. The US hotline has contact with the US industry and more than 130 companies across the world. Further, the US hotline publishes statics in their annual report about how much CSAM was reported to them per Internet platform. Also, both hotlines receive fundings and donations from the industry. Both hotlines see themselves to a lesser extent as a bridge between authorities and the industry. The Dutch, French, US, and EOKM adapt their processes to make it for the sector more convenient, for example, by not sending duplicate reports. The Canadian hotline is more on the other side of the spectrum. They do keep some contact with the industry to support them, but they are not adapting processes to make it more comfortable for the industry.

We became far more aggressive in terms of what we are going to send to companies. And I will be honest; we have plenty of complaints. We have people calling us spammers. We have been reported to anti-spamming groups. However, we are never actually listed as these notices are not spam." – Canadian Hotline

Concluding table

Table 6.2 summarizes the processes of the hotlines.

	(EOKM (NL Hotline)	UK Hotline (IWF)	Canadian Hotline	French Hotline	US Hotline
Reminders	Every 24 hours	After minutes, hours, dependent on the situation	Every 24 hours	Dependent on the situation	Every three days
Escalation	Domain registrar, law enforcement	law enforcement	law enforcement	law enforcement	law enforcement
Preventive instruments	HashCheckfilter	1.Blocking list 2.Preventive filter	Preventive filter	None	1. Hash-database 2. Industry platform, 3. CSE database
Fee for instruments	No	Yes	No	No	No
Relation industry	Medium close, national	Very close, national and international	Not close, national and US	Quite close, national	Medium close, national and international
Statics about companies	No	No	No	No	Yes
Proactive searching	No	Yes, manually and a targeted web crawler	Yes, manually, web crawler starting at known places and on the dark web	Manually	Manually
Mandatory or voluntarily reporting requirement of companies	Voluntarily, happens rarely	Voluntarily, happens rarely	Voluntarily, happens rarely	Voluntarily, but rare	Required national and international voluntarily

Table 6.2: Concluding table hotline processes

INHOPE

The direct role of the organization INHOPE in the international processing of CSAM is small. However, INHOPE facilitates the platform ICCAM. Members of INHOPE exchange all their reports through ICCAM. Suppose a hotline has found a CSAM URL hosted outside their territorial boundaries and within the jurisdictional territories of another INHOPE member. In that case, the hotline files the report in ICCAM. The hotline of the country where the URL is hosted gets a notification and can take action. The reporting hotline specifies the URL, the IP-address (and country), net name, other specifications, e.g., necessary references. There is no delay in filing a report and reporting it to the designated hotline. Many hotlines use Application Programming Interfaces (API) to automize the process of filling out and receiving reports. Currently, some of these APIs cannot fill out required fields in ICCAM, such as references. Consequently, hotlines need to fill out those fields manually which cause delays. In exceptional cases, reports get stuck in the ICCAM and are delayed.

6.2.2 *Hosting providers processes*

First, the general handling of abuse and, specifically, CSAM is described. Then, the hosting providers' efforts in the area of checking, monitoring, and sanctioning are discussed. Thirdly, preventive and proactive measures of the hosting providers are set out. Finally, a comparison to general abuse procedures is made. The table below shows an overview of the characteristics of the hosting providers as defined by themselves. It has to be noted that this is based on conducted interviews. Listed Hosting Providers can be datacenters without severs, IAAS parties providing datacenter and computing infrastructure (business2-business), and web hosting providers with a focus on a broader spectrum of smaller customers. Table 6.3 displays the characteristics of the hosting providers.

	HP1	HP2	HP3	HP4	HP5	HP6
Country of Registration	Netherlands	Netherlands	Netherlands	Netherlands	Netherlands	Netherlands
Number of customers approximal	5000	4000	230.000	9500	160.000	700
Number of IP-addresses approximal	6200	4200	No, rented from AWS	290.000	None, all sub-allocated	-
Storage space	Less than a couple hundred Terabytes	-	None	-	None	-
Own servers	Almost none	Almost none	None, all rented from AWS	Yes	None, all on Subsidiary name	None
Type of services	**Hosting and mere conduit** Mostly infrastructure: IP-addresses and bandwidth. Limited unmanaged dedicated services	**Hosting** Managed hosting, unmanaged hosting, virtual servicers, colocation and limited shared hosting	**Hosting** Shared hosting: web hosting, regular hosting, and e-commerce services	**Hosting and mere conduit** IaaS: unmanaged services, co-location, cloud, bandwidth, VPS	**Hosting** Webhosting in the form of shared hosting	**Mere conduit** Infrastructure: Co-location, unmanaged hosting
Access to network	Almost never direct access, only IP-addresses	Sometime access to network, often IP-addresses only	Total access to network of clients	Almost never direct access, only IP-addresses	Total access to network of clients	No access to the networks only IP-addresses
Receiving CSAM reports	Occasional, (max 3 p/m)	No	No	Yes	No idea	Occasionally (2 in 2020)
NL/Internation network/ customers	Predominantly international	Both Dutch and International	Mostly Dutch	Predominantly international	Both Dutch and international	Both Dutch and international
Dedicated abuse team	Yes	No	No	Yes	No	Mixed
Member of a sector organisation	Yes	Yes	Yes	Yes	No	Not an Hosting Sector industry organization
Classifies itself as hosting provider	Yes	Yes	Yes	Yes	Yes	No

Table 6.3: Overview of the characteristics of the hosting providers as defined by themselves }

General CSAM handling processes

In general, there are two different processes the participants follow. In the first one, applied by three hosters, the hoster intervenes after giving the client a chance to take down reported CSAM:

1. A report in the form of an e-mail is sent to the abuse-mailbox;
2. An automatic system creates a ticket based on the e-mail, e-mail topic, and the sender;
3. Suppose the automatic system recognizes the reporter, customer, and type of abuse. In that case, the ticket is automatically sent to the right customer, based on the IP-address and/or domain mentioned in the initial e-mail. Depending on the reporter and the type of abuse, the system sets a takedown time limit. For CSAM, that is one hour. However, if one of the fields is not recognized, it will be put in a queue for a manual check, and an employee will further handle it;
4. For some providers, after a notification is sent to the customer, the reporter is notified that the customer is notified by the provider;
5. If the customer has taken down the material, it is obligated to report back to the hosting provider within the set hour. For some, the customer must also explain why the material was hosted on their service or explain how the prevent this from happening again;
6. The hosting provider will then report back to a reporter that the material has been taken down. Some hosters also share the reason given by the client with the reporter.

HReports can be individual, companies or organisations. HP1 and HP2 systems categorize abuse based on the sender of the e-mail and secondly on the topic and the e-mail content. All e-mails of EOKM are automatically categorized as CSAM. The system of HP4 categorizes abuse based on keywords in the e-mail topic and text. All e-mails that indicate the hosting of CSAM will be categorized that way. The system of HP4 categorizes abuse based on keywords in the e-mail topic and text from any source. All e-mails that indicate the hosting of CSAM will be categorized that way. The systems use the combination of child+ certain keywords such abuse/misuse etc. To categorize a report, the combination of child+abuse has priority over other types of abuse. Without those keywords' reports will be handled manually. The e-mails of EOKM always include those keywords. Additionally, EOKM is a trusted notifier, and their reports are always forwarded automatically by the HP4 with a 1-hour deadline to remove the content. All hosting providers using the first process set a takedown time at one hour when reports are classified as CSAM. HP1 notes that if they receive an e-mail from another reporter than EOKM about CSAM, the notification is first sent to EOKM for a check.

HP1 also extra prioritizes reports if EOKM or the Dutch police (or other trusted organizations) indicates that the found material is very shocking. In that case, HP1 blocks the IP-address on which the URL is hosted immediately.

All interviewed hosters use a version of the process mentioned earlier and have their processes automated, for HP4 always with manual escalation where needed. If notifications can be categorized, there is no delay between receiving an abuse report and notifying the customer. If the report cannot be categorized, a notification needs to be sent manually, and this can only be done during working hours by an employee. HP2, a smaller provider, uses ABUSEIO for abuse handling, including CSAM. The system indicates for clients how urgent a report is on a scale; (1) Informational, (2) Needs to be solved, (3) It needs to be solved immediately.

Secondly, three participating hosters apply a process in which the hosters intervenes first and then informs the client:

1. A report is sent to the abuse-mailbox;

2. The report is assessed, and it is decided manually or automatically if a trusted flagger sent the report;

3. If so, the IP-address or service (e.g., domain) on which the content is hosted is taken offline;

4. The client is informed and is asked to take it down. The client also needs to explain;

5. If the client reports when the content is deleted, then the hoster unblocks the service;

HP3 checks if the material is taken down from the service before making the service online accessible again. The other hosters do not check but trust the message of their client. Only one hoster that predominantly provides Internet infrastructure instead of web hosting blocks the IP- address on which CSAM is hosted as soon as they receive a takedown request from EOKM. For this hoster, blocking the IP-address implicates the possibility that not only the services of the customer who hosted the CSAM are taken down but also the services of other clients. According to HP5, this can be up to 4000 customers.

The abuse handling of HP3 and HP5 is done manually by assigned employees. If they receive a notification from EOKM, an employee needs to manually take down the client's service on which CSAM is hosted. Abuse reports that are send by a trusted flagger like EOKM are prioritized. Taking down a domain takes a maximum of one working day. HP6 also performs some abuse handling actions manually. When HP5 gets a notification from EOKM, this notice is sent to more than 20 employees, from CEO to mailman. All receivers of this message can then "turn-off" the hosting IP-address. HP5 notes that this happens both during and outside office hours.

"We are not going to wait and hide behind the client in the way: "We gave it to a client, and if the client does not take action, we cannot do anything. Therefore, we will just block the IP-address" – HP5

In addition to the general processes, HP4 pointed out a particular case. For IP-addresses hosted through the network of Cloudflare, a slightly different process is in place for abuse handling.The moment a reporter looks up which hosting providers hosts an IP-address in a WHOis database, Cloudflare pop's up as hosting provider. However, Cloudflare only publishes the data through their IP-address and retrieves the data through the IP-address of the actual hoster. The processes which should be followed to handle abuse adequetly is:

1. The notifier fills out the abuse form of Cloudflare; they mention the IP-address of Cloudflare, the URL on which the content is hosted and why it should be taken down;

2. Cloudflare redirects this to the hosting provider with a reference number. The number is also shared with the notifier and adds the real IP-address of the hosting provider;

3. The hosting provider processes like any other abuse report.

However, reporters frequently do not follow the above-described process. Instead of filling out the Cloudflare abuse from the reports, they reach out to Cloudflare to determine which hosting provider is behind the domain. However, in this process Cloudflare provides the name of the hosting provider, but not an IP-address. The actual hosting provider is not able to find the affiliated client without the real IP-address. HP4 believes this is due to a lack of understanding at the reporter's side as the notifier does not understand that more information is needed to locate a client. However, HP4 does not encounter a problem with the Cloudflare process within EOKM.

(Contractual agreements on) checking, monitoring, and sanctioning

All hosters have contractual agreements with their clients about abuse handling. These agreements give hosters the right to cancel service due to non-compliance with the user policies. All user policies include that clients cannot host CSAM. An exception to this rule is when a client can prove it did not upload the material themselves. Such an exception is when a service is compromised/hacked. Some hosters also make an when the customer provides a service that allows user-generated content. The hosters using process one included in their user policies that the client needs to take down CSAM within one hour. Not complying with this rule is only acceptable for HP1 and HP3 if the client has a good reason for it, such as being in an airplane for a few hours. HP1 notes that if a client does not have a good reason, they terminate the contract. HP1 also stated that if the client does not respond within one hour, their support desk will call the client. If the client does not respond, the IP-address is blocked. If they do not respond after that, HP1 will terminate the service. If the client did not respond within an hour, it also needs a solid reason for HP1 to continue the agreement.

"After an hour, we will call and say "this is serious, would you like it if such a picture of your son or daughter would be online""- HP1

HP4 will end the services based on non-compliance with their user policies with a client if they are a repeating offender. The hoster has a definition for what a repeating hoster entails, but it is also dependent on the context in which the violation of user terms is made. If a client becomes a repeating offender predominantly depends on violating the time-limit and not having an acceptable reason for this.

"We had one client who would always let us know priorly of his vacations that he would be unreachable. He specified at which times he would be in the airplane and therefore not meet the time limit if abuse was reported. However, the moment he came online, he removed everything immediately. Of course, we will not cancel his services at that moment. "– HP4

HP6 also notes that in the case of repeated violations, it will end the customer agreement. Ending services or blocking an IP-address is a manual action for every hoster. HP1 is strict with the rule that clients do not only need to take down the material but also need to respond within the hour. Two hosters using process one only notes if something is taken offline if the customer reported back that they did. They do not double-check it. HP2 also trusts the client but states that they sometimes check a notification involving very severe abuse. HP1 is stringent that customers need to report back to them at all times. HP2 states that they need to report back in theory but is not very strict on that particular action. It is dependent on the severity of the abuse. Since the HP2 believes to have no cases of CSAM, they are not sure if it will apply for CSAM.

Furthermore, HP1 and HP4 always report back to the reporter about the undertaken steps. HP4 adds that it is also the reporter's responsibility, in general, to send a reminder if the material is not taken down. However, for CSAM, they manually check themselves after 1 hour if the content is truly removed. If the content in not removed HP4 will also block the service. The customer approach of HP2 is less based on checking compliance of the user policy but more as a personal approach. If HP2 frequently receive abuse reports for a specific hoster, they will reach out to them. In that conversation, they address the current state of affairs and which measures should be implemented to perform better in the future.

"In the case of a new starting customer with much abuse, the hoster will start a conversation and say, "You are not able to handle it, how can we help you to get it under control?" – HP2

The user agreements and activities on monitoring, checking, and sanctioning are slightly different for the hosters using process 2. The user agreements describe that in the case of a client hosting CSAM, the concerned service is immediately blocked. Unlike the other hosters, HP3 and HP5 always check if the material is taken down before putting a service online again. HP3 notes that because the largest share of customers is end-customers, they often do not understand that they are responsible for monitoring and securing their services. The lack of understanding sometimes leads to a situation in which HP3 is asked to help the customers.

Proactive or Preventive filtering

Only the customers of HP4 and HP5 use the HashCheckServive. The other hosters would consider letting Webhosting services/image hosters use the HCS if those services receive reports on CSAM regularly. HP6 underlines that they will only use the HCS if it fits easily into their day-to-day business.

HP4 laid down contractually that all customers who host websites where content is user-generated are obligated to use the HashCheckservice. In practice, HP4 only asks clients who received reports immediately, to use and implement the service whether it is their first report or not. These are predominantly re-sellers with clients with platforms that offer space for user-generated content. HP5 also obligates customers to use the HashCheckService when receiving reports about CSAM regularly. HP5 built a platform on which the HCS and other security services is operated. Clients are obligated to implement this platform. This obligation is not contractual, but HP5 does enforce it by cancelling the service.

"If the client does not want to implement the HashCheckFilter, we will cancel the customer agreement and the services immediately. The client maybe says, "you cannot do that. I go to court", but if you do not want to do it, we know you have bad intentions, and we are willing to take the lawsuit" – HP5

HP6 uses a system that checks the domain names of clients on specific terms or typos. If the system marks all domains with typos and high-risk words, an employee will look into it. If it is a false positive, nothing happens. If it is correct, the service is taken offline until the customer has explained it and changed it.

Pre-verification of customers or Know-your-customer procedure

Four of the six hosting providers have a pre-verification system for customers. All those hosters predominantly offer Internet infrastructure instead of Webhosting. The two web hosters HP3 and HP6, do not have any pre-verification system for their clients; the only requirement is that customers need to pay with Ideal of a credit card. The systems of the four hosters with a pre-verification system is based on different elements. The automatic system of HP1 compares the geolocation of the IP-address with the county filled out by the customer. If those two are not corresponding, the application is stopped. When they correspond, the system also checks if the person or company is registered on the blacklist of Fraudrecord.com. If so, the application is stopped. Frauderecord.com is a website that provides a list of hashed customer information of customers with a criminal history.

Similar to the procedure of HP1, in the Know-Your-Customer (KYC) procedure of HP4, an automatic system checks several points of information of the customer order and filled in customer information. The automated tool checks the geolocation, phone number, address validity and whether those three pieces of information have a mismatch in the country information (for example, an NL IP with a US address and a phone number from Ukraine). The address is checked for validity, and the company name is screened for key words. The payment method is verified and checked for potential fraud. Duplicate accounts and previously terminated accounts are also automatically checked, for example if the new customer is a previous bad customer. If certain information does not match or is red flagged, the customer is reviewed manually by an employee. In certain cases, an employee will further reach out to the potential client for an extra verification process where more information can be requested, such as an extract from the Commercial Register of the Chamber of Commerce or an international equivalent. Next to that, HP4 also keeps track of embargoed countries, has their own blacklist of terminated customers and implemented specific processes for countries where abuse is more likely to be an issue. Additionally, certain types of businesses require extra verification from the start, such as Cloud Storage Providers. They will receive a questionnaire, where they fill out and confirm by signing that they have an anti-CSAM policy.

The pre-verification process of HP2 is based on the process proposed in the M3AAWG anti-abuse whitepaper. The elements of the procedure are: Know-your-customer and being careful with the automatic supply of services. Further, HP2 believes that their zero-tolerance reputation and strict abuse policies lead to self-selection under potential clients. Potential clients with bad intentions are less likely to take a service at HP2. The pre-verification procedure of HP5 includes that all co-location customers need to ask to enclose a copy of an extract from the Commercial Register of the Chamber of Commerce or an international equivalent to their service request.

The pre-verification process of HP2 is based on the process proposed in the M3AAWG anti-abuse whitepaper. The elements of the procedure are: Know-your-customer and being careful with the automatic supply of services. Further, HP2 believes that their zero-tolerance reputation and strict abuse policies lead to self-selection under potential clients. Potential clients with bad intentions are less likely to take a service at HP2. The pre-verification of customer procedure of HP5 includes that all co-location customers need to ask to enclose a copy of an extract from the Commercial Register of the Chamber of Commerce or an international equivalent to their service request.

General abuse

For all hosters, the handling of abuse is the analogous to the handling of CSAM. The difference lies in the manual check of "non-trusted" flaggers, the prioritization, and the given time limit for clients to take it down. Furthermore, HP5 immediately blocks an IP-address if CSAM is reported but doesn't for other forms of abuse. The given time-limit is between 1 and 24 hours. Also, for other abuse, it applies that if the police or another trusted flagger indicates that the material is exceptionally harmful, the hosters will act right away. HP1 has a strict rule that the customers always need to respond to the hoster, and they send it back to the reporter. HP4 also requires a response or an action taken and marked by the customer via HP4's in-house developed abuse handling system. If a customer fails to act within the given deadline, their involved IP addresses will be null routed. If the customer explains how the abuse is resolved and confirms it is truly resolved, the IP address will be released again.

"The explanation of the client is always shared with the report. To confirm that we are processing it and then also that the abuse is taken down off the Internet. The reporter knows that it does not end in a black hole. We believe it is decent to do and also with other people do the same for us." – HP1 For general abuse

reported by non-trusted flaggers, all hosting providers perform a manual check. Besides, HP4 accepts all received abuse notifications, whether from trusted or non-confirmed trusted flaggers. Therefore, there are no obstacles to report an abuse notification. HP6 noted that notifications of non- trusted flaggers are often ignored. Depending on the beliefs of the provider, something is considered illegal or harmful and taken offline. HP3 highlights that they find freedom of expression so crucial that they even paid the legal representation of a sued client. This hoster also included that if an employee is unsure about a takedown request's lawfulness, the company board is consulted.

"The client had a blog on which he published caricatures of a famous cartoon character. The company of the cartoon character demanded that the content should be taken down. The client did not have the money to fight this company in court. Nevertheless, since we believe freedom of expression is extremely important, we offered paid layers and other secondary costs. Eventually, this client won 4 out of 5 points of the lawsuit" - HP3

For the takedown time limits, HP5 points to the law, which says that content needs to be taken down in a "reasonable" time. Accordingly, the hosting provider always looks at the context when setting limits. The hosting provider considers the client's number of employees, how many steps are there between the client and the end-user, and the customer's general experience. However, when receiving a notification of CSAM the hoster will immediately block the IP-address of the customer. All other hosters also address that for general abuse handling, the take downtime limit and the consequences are dependent on the type of abuse and other contextual factors. HP1 addresses that in the case of a spam report, they expect the same response time as CSAM. At the same time, copyright infringement has a much lower priority. Also, HP2 has a prioritization scheme for abuse handling. For vulnerability notices, HP2 does not expect any action at all.

Multiple hosters mention that their clients always need to respond to every abuse report. This can be to the hoster or the reporter. HP6 tells that the contact will be directly between the client and the reporter, and only if the client does not respond that a report can ask them for help. Most hosters turn of the IP-address and then terminate the contract if the client does not respond to abuse notifications. Two hosters specify that they always report back to the original reporter.

Concluding table

Table 6.4 summarizes the processes of the hosting providers.

	HP1	**HP2**	**HP3**	**HP4**	**HP5**	**HP6**
Customer Takedown time	One hour	One hour	Service taken down immediately	One hour	IP-addresses immediately blocked	Service taken down immediately
Prioritization based on	Trusted flaggers	Trusted flaggers	Keywords in the notification and trusted flaggers	Trusted flaggers	Trusted flaggers	Trusted flaggers
Monitoring of reports	Based on customer repsonse	Based on customer response	-	Based on customer response	-	-
Automatized abuse system	Yes	Yes	No	Yes	Yes	No
Checking	No	Yes	No	Yes	No	Yes
Customers reporting back	Yes strict	Not strict	Yes, until then service remains offline	Yes, strict	Yes, until then service remains offline	Yes, until then service remains offline
Proactive checking	No	No	No	Yes: HCS	Yes: HCS	Yes: domain names
Customer pre-verification	Geo-location match & fraudrecord.com	M3AAGW policies	No	Geo-location, phone number, address validity, payment method, possible an extract from the chamber of commerce	No	Extract from the Chamber of Commerce or equivalent
General abuse procedures	Similar	Similar	Similar	Similar	Similar	Similar, only never immediate IP-blocking

Table 6.4: Concluding table hosting providers NTD processes

6.2.3 *Dutch specialized force child abuse*

TBKK consists of regional teams and a national team. The regional teams are predominantly focused on investigating and local engagements. The work of the national team is divided into three pillars. 1. Information streams, 2. International contacts, and 3. Investigating the Dark web. They also hold a role in the NTD process, but this is just a small portion of their work.

Investigating information streams

In this pillar, the police aggregates report of CSAM and related information like accounts, IP- addresses, and e-mail addresses. It is important to note that the police will not issue takedown orders for this but will use it to see if they have enough information to start an investigation. NCMEC provides most of the information gathered by the police. Every day the police receive around 30 to 50 reports of NCMEC. All content or information is in some way affiliated with the Netherlands. These reports come from the industry, which has a legal reporting duty in the United States. Companies who report to NCMEC already deleted this content themselves. Sometimes platforms delete whole accounts. Therefore, issuing a takedown order is not necessary. Another information stream is gathered in an internal mailbox. The public can report here. Also, the reports EOKM deemed suspicious are gathered there. However, the police note that this is just a small part of the information stream and that the primary source is NCMEC. The police assess all evidence and search for a prospect of conviction. If they cannot immediately find something, it will be saved into a database for investigations, possibly later on. Without a reasonable prospect of conviction, the police cannot write a convincing report, and the state's attorney will not permit to start a further investigation.

Liaising with International (law enforcement) agencies

This pillar is mostly focused on Child Sexual Abuse tourism. The Dutch Police gets reports from Dutch people who abuse children abroad. This pillar also includes an international program in which information is gathered to start international law enforcement investigations.

Dark web investigation

This last pillar focuses on all activities on the dark web, which are affiliated with CSAM. Aimed at frustrating offenders and start to gather enough information to start investigations.

Role in the Notice-and-takedown

The police act as an escalation step for EOKM. If hosting providers do not comply with the requests of EOKM, the police can also send a takedown order. There are a few other reasons why EOKM asks the police to send a takedown order to hosting providers. However, these reasons are sensitive and cannot be outlined in this report. The police send between 10 to 4000 reports per month to hosting providers.

Moreover, the police maintain and owns the database used by EOKM to check images and provide the HashCheckService to the industry. The police added several databases to their database and are continuously expanding it. At this moment, the hash database consists of 1,5 million hashes. The hash's included in the database at least checked by three people. In that way, it is assured that the hashes are illegal and old CSAM. The hash database is expanded every two months with around 100.000 hashes.

The database consists of the Dutch law enforcement database and is configurated with the database of the law enforcement agencies of the UK, the US and Canada, and Europol. It only includes images from already closed cases. In the current database, only images are included and not videos. Because videos are easily altered from which the hashes become useless.

Investigating bad hosters

Not often, the reports are used for investigation hosting providers. But in some cases, reports are also used for starting criminal investigations against individuals.

7

Results 2: Stakeholder perspectives and the combined qualitative and quantitative results

Sub-question 2

Who are the relevant stakeholders, and what is their position regarding the government policies to clean the Internet of CSAM?

This chapter continues to discuss the quantitative results and sub-questions 2,3,4 and 5 are answered. The first section sets-out the stakeholder positions. Secondly, the participation of the stakeholders in the policy-making process for the government policies is discussed. Then. the stakeholder's evaluation of the government policies is displayed in section 3. In section 4 the quantitative and qualitative results are combined. Finally, section 5 reflects on the improvement's stakeholders proposed.

7.1 Stakeholder positions

The positions of the stakeholders on the government policies are discussed below. The stakeholders' position on the government policies can be derived from their mission and motivation for this policy field, displayed in table 7.1.

The missions of the stakeholders are all positively aimed at cleaning the Internet of CSAM. Although they are quite overlapping, they are significantly different on one significant element. The Industry representative, the Ministry of EZK, the RIPE community, and most of the hosting providers point that government policies should not compromise the sector's economic welfare (too much). The other stakeholders do not mention avoiding economic risks as their core goal.

The Ministry of EZK, the Ministry of J&V, and TBKK have a legal obligation to develop or execute government policies. All other stakeholders are mainly driven by societal duty. This crime's egregious character against children motivates companies and organizations to participate in government policies and the affiliated processes. Almost all stakeholders named reputational risks as an incentive. However, it differs per stakeholder whose reputation they keep in mind. The Ministry of J&V and EZK strive for a good reputation of the Netherlands in Europe. The EC defends the reputation of the European Union

Stakeholder	Policy objective	Motivation
Ministry of J&V	Bring down the total volume of hosted CSAM on Dutch infrastructure.	Societal duty, legal mandate, reputation
Ministry of EZK	Bring the volume of CSAM down without economically compromising the sector	Societal duty, reputation
European Commission	Decreasing the total volume of CSAM in Europe.	Societal duty, reputation
Hotlines	Decrease or even erase all CSAM of the Internet.	Societal duty
Hosting providers	Taking down reported material as soon as possible and prevent material from being uploaded.	Societal duty, reputation,
INHOPE	Supporting CSAM hotlines	Societal duty
TBKK	Detecting child abuse, saving children from ongoing abuse situations and play a key role in the prosecution of offenders.	Societal duty and legal mandate
Industry representatives	Represent the industry towards the government as good as possible while also striving for a safer in internet for children	Societal duty, reputation
Community RIPE NCC	Do what is good for all	Societal duty

Table 7.1: Stakeholder objectives

in the world. The industry representative wants a good reputation of the sector globally, and the hosting providers fear their reputation towards their clients and in general.

It is notable that although hosting providers also have a legal obligation to take down material, none of the participants have named legal obligations as a driving factor to participate in government policies (European Parliament, 2000). Also, the absence of financial incentives is remarkable.

Furthermore, the core business of the UK, US, and Canadian hotline is split up into cleaning the Internet of CSAM and activities regarding missing Children and victims. Hence, their perspective is sometimes more victim-focused than from the Dutch and French hotline. Although they have primarily the same goal, the perspective of how to reach it differs.

7.2 Stakeholder participation in the Policy-making process

Sub-question 3

How do the relevant stakeholders participate in the policymaking process?

Stakeholders participate in the policy-making process in a policy-arena. Two relevant policy-arenas can be distinguished: the policy-arena of the government policies and the policy-arena of the EC policies. Because the EC's policies directly influence the Dutch policies, it is essential to consider them both. Next to these policy arenas, there are also a few composed actors. Composed actors are stakeholders consisting of several or many individual organizations. The decision-making processes within these organizations are discussed shortly.

How stakeholders participate in the policy-making process is dependent on their position towards the government policies. The way stakeholders participate is also influenced by the instruments they must influence in the process and their dependency on another stakeholder. The position, instruments, and dependency translate into a strategy that stakeholders knowingly or unknowingly apply. At first, the perceived dependency is discussed. Secondly, the strategies of the actors are presented. At last, the relations between the actors are shown.

7.2.1 *Perceived dependency*

The Ministry of J&V and the Ministry of EZK perceive an interdependency. Both ministries need to agree on letters and policies. The Ministry of EZK does feel that because the Ministry of J&V is in the lead, they are a bit more dependent than the other way around. Since J&V took the leadership in the policy-making process, they have the agenda-setting power. Interesting is that the Ministries have a different outlook on the dependency of the Government on the industry. The Ministry of J&V believes it is good to work together with the industry but does not believe they are entirely dependent on the industry. The current policies fall or break with the hosting providers' voluntary efforts, but with the administrative authority's introduction, the Government can enforce it. Contrary to the Ministry of J&V, EZK believes that collaboration with the industry is indispensable for the approach.

In general, the industry perceives a high dependency on the Dutch Government due to the Government's legislative power and public legitimacy. However, some companies believe only to need to follow government policies if they agree with them. In those cases, the perceived dependency is lower. The hosting providers also generally feel dependent on the industry representatives because they have a seat at the table. Furthermore, two hosting providers also do not believe they are dependent on the government. They have the feeling that government regulations, if not reasonable, are not relevant. The other hosting providers believe they are dependent on the government as the government can introduce laws and damage their reputation. The industry representatives perceive a high dependency on the Government. There is not an interdependency between the industry representatives and the Government. However, the Government acknowledges being dependent on the industry representative as they are the industry's gateway.

There is also a perceived interdependency between the Dutch hotline and the Government. The Dutch hotline performs indispensable tasks, and the Government provides financial resources. Furthermore, are also the legislative and enforcing efforts vital for the Dutch hotline to function. Moreover, does EOKM believe to be dependent on the hosting providers for taking down the content and implementing preventive measures.

On an international level hotline, the Dutch Government and INHOPE perceive a dependency on the EC. RIPE NCC does not feel dependent on the EC right now but believes to be in the future as Government will be more involved in this part of governance.

The perceived dependency of hotlines on the hosting sector is correlated with how reliant they are on their financial support. The hotlines have different income models. The higher the dependency on financial resources, the higher the perceived dependency. In general, hotlines feel financially dependent on other stakeholders or actors.

7.2.2 *Perspective on responsibility*

The stakeholders have different views on who is responsible for what in the government policies. Most stakeholders believe there is a shared responsibility between all stakeholders, although the government and the industry are named as predominantly responsible. The Ministry of Jis on the other part of the perspective and believes the sector is responsible for the cleaning of the Internet and prevention efforts. However, since the industry failed, the government must step in.

The perspective of hosters on responsibility is different. A few hosters have addressed that their responsibility lays solely in complying to set norms and laws. However, the hosters implement procedures that are more far-reaching that are out of the scope of their responsibility and they believe it is their duty to do that. Other hosters note that due to the lack of access to the networks of clients the government cannot expect them to take it down without providing the necessary instruments and cannot expected them to do anything possibly compromising their profits. The stakeholders disagree on who is responsible for financing the government policies. More than half of the stakeholders believe that the hosting sector should predominantly pay for the (development of the) instruments. The sector profits from the services that create the problem and should therefore pay for it. Just one hoster shares this few and believes that because they make a substantial income/profit, they can be expected to pay a part of the instruments necessary to clean the Internet. The instruments concerning enforcement and part of the Dutch hotline activities should be paid for by the government. This because these activities are considered the responsibility of law enforcement. If the Dutch hotline does not do it, the police need to do it, which is much more expensive.

Actor strategies

Table 7.2 displays the resources and strategies the stakeholders apply to pursue their policy objective. Interesting to note is that only the Ministry of J&V shows an offensive strategy, and, on some occasions, the Dutch hotline does too. All other stakeholders do not actively persue their objectives by initiating policies. The reactive or proactive strategy seems to correlate to the perceived dependency. Only the Ministry of J&V and the Dutch hotline perceive a low dependency on other stakeholders. The Ministry of J&V seems to be the driving force behind the establishment of government policies. Most of the current government policies are established in the PPC. However, the Ministry of J&V is also the initiator and driving force behind this partnership. Hence, other stakeholders do mostly react to proposed policies or identified problems.

Moreover, The PPC and close contacts between the stakeholders indicate an interactive strategy of the stakeholders within the PPC. The renewed approach was established in collaboration with the PPC. However, the Ministry of J&V, hosting providers, and Industry representatives sometimes behave according to an autonomous strategy. These stakeholders do not always seek collaboration. The Ministry of J&V introducing a duty of care policy without involving the PPC reflects an autonomous strategy. Also, the Industry representatives fending off the duty of care is an example of autonomous behavior. Moreover, some hosting providers demonstrate autonomous behavior by not implementing policies when disagreeing.

Organization	Strategy	Resources
Ministry of J&V	Offensive and hybrid autonomous and interactive	Formal power, information, position in the network, money (to a small extent)
Ministry of EZK	Reactive and interactive	Formal power, money, position in the network , information
European Commission	Offensive and Autonomous perpetuation	Formal power, money, manpower
Dutch hotline	Hybrid reactive and offensive and interactive	Knowledge, indispensable role
Foreign hotlines	Reactive and interactive	Knowledge
Hosting providers	Reactive and often autonomous, sometimes interactive	Implementation power, knowledge
INHOPE	Reactive and Interactive	Knowledge, position in the network
TBKK	Reactive and Interactive	Position in the network, indispensable role
Industry representatives	Reactive and hybrid autonomous and interactive	Knowledge, position in the network
RIPE NCC	Reactive	Knowledge, position in the network

Table 7.2: Stakeholder strategies and resources

7.2.3 *Relations between actors and influence on the policy-making process*

The stakeholders have informal and formal relations through which they can influence each other. The actors with a direct influence on the government policies are limited to Dutch actors. The European Commission can steer the policies but only through formal and somewhat distant activities.

The Dutch stakeholders identified the PPC as the leading platform on which the Government, industry, and Dutch hotline can influence each other. The hosting providers influence the Government through the industry representatives. However not all hosting providers are members of industry organizations. In that case, the Government can only influence hosting providers through laws and political pressure and hosting providers cannot reach the Government.

The majority of the hosters do not feel heard and believe in having little influence on the policies, mainly caused by the belief that the industry representatives are not capable of defending their interests. This dissatisfaction originates from a high perceived dependency on the Government and Industry representatives. Arguments for the industry representatives' inability are their lack of influence and that they are not a reflection of the sector. Mainly due to a low organizational degree within the sector. On the other hand, one hoster also noted that many companies are still not interested in participating in the policy-making process on both Government and EC levels.

Moreover, also the industry representatives are dissatisfied with their possibilities to influence the government policies. They believe that the Ministry of J&V is incapable of committing to a public-private partnership in terms of shared responsibility. The inability to commit is the consequence of the sometimes-autonomous strategy of the Ministry of J&V. Two industry representatives reasoned that Minister Grap-

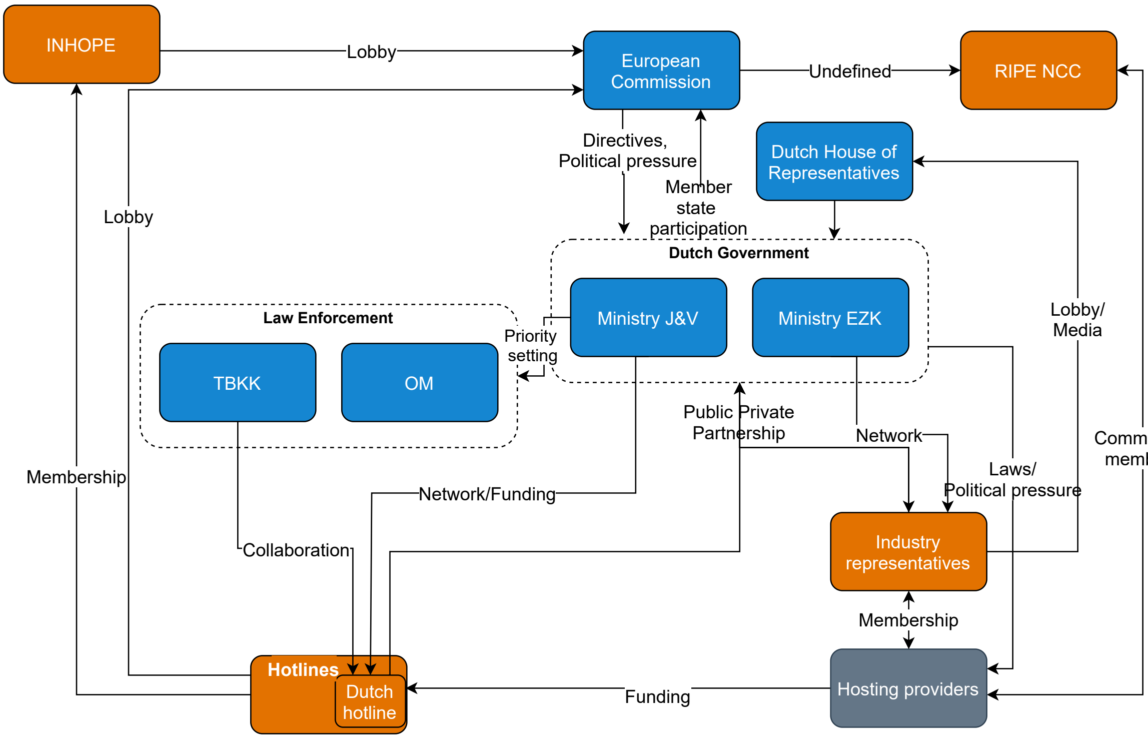

Figure 7.1: Informal and formal relations between the stakeholders

perhaus takes too much credit for the sector's work, does not publicly appreciate their efforts, and says things in public that are conflicting with what is discussed and agreed to in the PPC. Secondly, the representatives believe it is highly inappropriate that Minister Grapperhaus introduced a new regulation (Duty of care) in the naming-and-shaming letter to the parliament without previously consulting the PPC. They feel it as a stab in the back and is outrageous to do while being in close cooperation. The only other way for industry representatives to influence the Government is via the Dutch House of Representatives. However, this hasn't been practiced in the past.

"In the public-private partnership, four action lines were formulated. The sector did not even support every measure, but we decided to work along with the Ministry. We always said if it just these four, we want to help. Because it is an important topic and we want to give input although there are two action lines, we are not happy about. We put a lot of effort into forming these policies and implementing them. And then you see that in the letter to the parliament, the minister writes, "I have this program, and I did that in the PPC. Now I am going to take more action, but I will leave the sector completely out of it." I find that inappropriate" - Industry Representative

On the other hand, the Dutch hotline is happy with the current level of participation in the policy-making process of the government policies.

Hosting providers do not exercise direct influence on hotlines. However, when hotlines feel they are more dependent on hosting providers, their behavior seems to be influenced. The Dutch, French, US, and UK hotlines are all, to a certain extent, financially dependent on the sector. They all believe that a good with the sector is essential to be effective. The Canadian hotline is not financially dependent on the sector and believes a good relationship is not vital for their work. Furthermore, the hotlines do all share one objective. However, due to their financial dependency, the hotlines need to protect their relevance. Sharing services, techniques, and all information are therefore often disputed.

The policy-making process of the EC policies is more international focused. Notable is that although INHOPE is the hotlines' umbrella organization, all hotlines undertake individually lobbying or information providing activities. Their efforts are on that level not coordinated. Because the hotlines have different perspectives on the EC policies, they will advocate for different things. An example is the interfering with encryption and peer-to-peer networks. EOKM is very hesitant in that matter while the Canadian hotline is convinced that interfering with encryption and peer-to-peer networks would be essential to help children

The industry representatives sometimes participate in online consultations, but it is unclear how often this happens and what the influence exactly is. That means that the Dutch Government is the primary channel for the industry to participate in the EC policy-making process. Hosting providers confirmed that the sector's largest share is not even interested in participating. The Ministry of JV influences the European Union through official lines like the Justice and Home Affairs Council and diplomatic efforts of the Permanent Representation of the Netherlands to the EU in Brussels. The diplomats at the PR in Brussels oversee the activities towards the EU and have a big influence on the policies, within the rough lines sketched by the Ministries in the Hague.

The RIPE NCC community has an unclear influence on the EC. There are meetings, but the content of those meetings is not public.

7.3 Stakeholder evaluation of the government policies

Sub-question 4

How do the stakeholders evaluate the current government policies?

In this section, it is discussed how the stakeholders assess the current government policies and their effects. It is also discussed if the PPC stakeholders expected these effects. Specifically the naming-and-shaming policy is examined more elaborately. Both elements that are believed to have a positive impact and (potential) pitfalls, are considered. Positive elements are important to identify so they can be maintained or strengthened in future policies. Pitfalls will be used to weigh the relevance of improvements. In line with the research question, the focus lies on the Dutch government policies. However, since the EC policies significantly influence the Dutch policies, a more international perspective is considered. For the government policies, the four lines; 1. Transparency, 2. Self-regulation 3. Providing action perspective and 4. The administrative authority is considered separately. The policies that are already announced and in the process of implementation are not discussed in this section.

This whole chapter is written based on the perception of the actors. Because a qualitative and exploring research method is applied, the importance of findings cannot be weighted by the number of stakeholders mentioning certain elements. However, the number of stakeholders mentioning certain elements can be used to analyze the sentiment among stakeholders.

7.3.1 *Overall evaluation*

Overall, it is observed that most of the stakeholders believe that the (announced) government policies are, in essence, sufficient but that the current quality and execution is not yet adequate. Consequently, stakeholders trust the Government's policy lines but are convinced the policies need to be strengthened. Most hosting providers have a dissenting opinion of the other stakeholders. They are dissatisfied with the government policies and do consider them as sufficient or adequate.

Furthermore, regardless of the effects of the government policies, the appointment of Minister Grapperhaus is defined as a game-changing event. Minister Grapperhaus prioritized the fight against CSAM, providing financial resources for the Government and Dutch hotline and expanding civil servants' capacity. On a national and European level, stakeholders observed that the devotion of Minister Grapperhaus has moved the needle.

Most stakeholders know how the NTD mechanism works but do not have a strong opinion about other stakeholders' performance other than their classification group. Hosting providers do have an opinion about the sector in general but not about how the hotlines perform. Hence, the evaluation of specific roles is predominantly based on the perception of a small group.

7.3.2 *Transparency - Naming-and-Shaming*

The two main elements of the naming-and-shaming policy are discussed in this part separately. First the HCS is addressed and after the TU Delft monitor report.

The HashCheckService is embraced after the "warning letters."

In general, the effects of the "warning letters" were in line with what was expected. Stakeholders observed that multiple companies took deliberate action to improve their processes. The Dutch hotline was even positively surprised. Hosters reached out to EOKM to implement the HashCheckService. One hoster made the HCS mandatory for its customers and noticed that customers (re-sellers) removed their customers (domains) with a high volume of reports from their network instead of implementing the HCS, which is an even better result. The "warning" letters possibly caused a significant increase of checked and found CSAM by the HashCheckService. Hosting providers and industry representatives were less charmed by the warning letter. They believe it did not recognize the efforts of (some) of the hosting providers and caused confusion. This confusion made the Industry doubt the accuracy of the research.

No direct effects of the publication of the TU Delft report can be determined

Making the TU Delft monitor report public seemed to have less effect than the warning letters. The stakeholders did not observe any changes in terms of companies reaching out, plugging into the HCS, or taking other actions. Immediately after the publication of the report and the Government's letter to the House of Representatives, there was a bit of fuss in the sector. Two companies were angry and disappointed. There was also the rumor that a datacenter wanted to terminate its contract with a bad performing hosting provider. However, any real changes were not noticed by the stakeholders. Hence, the effect was not in line with the expectations. Both, hosting providers and industry, also doubted the research's trustworthiness and the legitimacy of making the report public. Used data would be incorrect by mistakes of EOKM, and Instruments were not developed enough yet.

The industry representative, the Ministry of EZK believe that hoster HP4, is unfairly named in the TU

Delft report. This was confirmed by a this hoster HP4 who believed to be unfairly called out for being non-compliant while, according to their data, they were proven to be compliant. According to the hoster HP4, some URLs were marked by EOKM as taken offline after 48 hours, while in reality this concerned a notification that was sent on Friday afternoon. EOKM's automated system did not mark that the URLs are offline, and since EOKM does not work during the weekends, these URLs were checked on Monday and then confirmed as taken offline. Due to the weekend in-between, they marked the URLs as 48 hours, while the URLs were taken offline within 1 hour. Accordingly, in the data, it seems like the hoster HP4 did not take down all URLs' within 24 hours, while the hoster could proof their customer took the URLs down within even 20 minutes.

"I asked somebody who is closely affiliated with the whole monitoring whether TU Delft had found something on our network, and this person told me we do not host CSAM. Then there is also no reason for us to apply a filter or anything. We will start seriously considering that if we get a notification." – Hosting provider

The initial objective was to create a benchmarking instrument for the industry with the TU Delft monitor. However, the stakeholders did not observe that the warning letters or the TU Delft monitor report led to a benchmarking among the hosting providers. The companies were fixated on how the Government assessed their performance, and they did not doubt their performance. It only hurt the trust of the hosting providers in the government. Hosters that did not receive a letter or were named in the TU Delft monitor report even saw this as a confirmation that they do not need to take any action.

7.3.3 *Self-regulation*

The self-regulation focused predominantly on the Notice-and-Takedown mechanism and especially the role of the hosting providers. This part discusses the evaluation of the integral NTD mechanism.

Too little CSAM is found, and there is a high dependency on Anglo-Saxon countries

Within the current system, stakeholders are convinced that only the tip of the iceberg of CSAM is found, which is labeled alarming. Besides, both the EC as the industry representatives believe it is undesirable that most CSAM is found by Anglo-Saxon countries' hotlines. The EC believes Anglo-Saxon countries find more due to mandatory reporting requirements in the US. While others believe it is due to the proactive searching activities of Anglo-Saxon hotlines. Both statements focus on different types of reports. NCMEC aggregates already taken down content, while the other hotlines aggregate still online URI's with content. It is undesirable as it poses a risk that Anglo-Saxon countries lay outside the influence sphere of the EU. Within the EU, hotlines are required to join INHOPE and commit to the agreements to get funding from the EC. Anglo-Saxon countries are outside that scope and can therefore decide about their activities; the Canadian hotline exactly did that. The transparency of the activities of hotlines is also limited. Secondly, the EC is also convinced that the EU as world power should deal with her own problems and therefore, should not be dependent on non-EU countries.

Automation of systems lacks behind and causes back-logs

It is recognized that the internal processes of the hotlines can improve. Hotlines are struggling with great amounts of CSAM, and it is not rare that organizations build up a back-log of notifications. Hotlines need a lot of human capacity, for which they do not have the necessary financial resources, as systems are often not automated. The technologies used for automation are also widely praised and believed to have a significant positive impact. Hotlines are also not that eager to share technologies because of the competition between them. It is also brought up that there are too many redundant steps in the process, from finding to taking down material.

Disputed if the performance of hosting providers can be evaluated well or not

Most stakeholders used the TU Delft monitor as a source to measure the hosting provider's performance. It is interesting to note that although the stakeholders have relatively similar objectives, the measurement of hosting provider's performance is significantly different. The Ministry of JV, the police, and other organizations that solely focus on the child's well-being believe a score of 84% taken down within 24 hours is a good start but certainly not sufficient. While other stakeholders like the industry (representatives) and the Ministry of EZK are also concerned with economic welfare, they see a score of 84% as quite well for self-regulation efforts. Consequently, it depends on which stakeholder is asked if they believe the hosting provider's current performance in the NTD mechanism is good or not. Notable is that all interviewed hosting providers believed that their processes were sufficient.

Low adaptation grade of self-regulation efforts

Besides the measured performance, do the stakeholders also have a view on how, in general, hosting providers comply with the self-regulation. It is expected that the self-regulation policies and agreements are not widespread among the hosting providers in the Netherlands. Only a small part of the sector is a member of an industry organization. Policies and self-regulation efforts will often do not reach them. Even among the members of industry organizations, it is believed that many members are not aware of the self-regulation efforts. Moreover, best-practices are rarely shared among hosting providers, holding back a sector-wide development and adaptation of effective processes.

Lack of differentiation between companies in the procedures and norms

Finally, the Code-of-Conduct and norms are all generalized for all companies operating IP-addresses, with little differentiation of the high variety of hosting services and mere conduit services. The performance of hosting provider is also measured the same for every company. Hosting providers addressed that such classification does not acknowledge the different possibilities hosting providers have. Consequently, such generalized processes are infeasible for some or ask much more efforts to reach the same outcome. Companies feel this as unfair and think it is counter-productive for the optimizations of processes. The self-regulation procedures been followed by the government. Therefore, the government is also generalizing all types of hosting providers.

7.3.4 *Providing action perspective*

All Dutch stakeholders noted that the current instrument could and should be improved to have a significant impact. Especially the HCS has much potential looking at the currently found images. Many improvements are already implemented or will be in the short future. Further, it is also expected that more can be done to prevent CSAM from getting uploaded online. The stakeholders disagree about what kind of measures, like a Know-Your-Customer policy, will be effective and proportional.

Doubts about the sufficiency of the instruments to improve the performance of companies

"You think you do everything right. You cooperate with EOKM and believe you have everything implemented that is possible. But then the message is that it is not good enough, and you do not really

understand why. Yes, that is frustrating" – Hosting provider

The Dutch Government, Police, and hotline all believe the current instruments are sufficient to judge companies' performance fairly. The industry, however, disagrees to that statement. They believe the perspective of action is too limited and unclear to publish the performance of companies. Hosting providers feel lost in what they can do to comply with the norms of the Dutch Government. An important factor here is that some hosting providers believed to have a close contact with EOKM but still found out later that their processes where not yet good enough. Consequently, they question the professionality of EOKM. According to EOKM the hosting providers do not always follow their suggestions.

7.3.5 *Regulation by an Administrative authority*

The administrative authority regulation is hard to evaluate as it is not implemented yet. However, stakeholders have opinions about the chosen approach and the announced elements.

All PPC participants believe the administrative authority will have a positive impact on companies' compliance. It is a relatively fast way of evoking pain to violating companies and compel them to comply. Currently, there are not many ways to enforce companies to implement preventive instruments and meet the 24-hour norms.

On the contrary, the hosting providers believe an administrative authority will not be effective and even counterproductive. The administrative authority will only issue fines, while non-compliant companies should be terminated, and affiliated persons are brought to justice. The current focus would lay too much on sloppy-hosters instead of bad hosters.

7.3.6 *Overarching pitfalls of the current Government policy*

Some pitfalls of the current Government policy are overarching and affect multiple policy lines. Those are discussed below.

Lacking representation of a large share of the sector

The low organizational degree of the hosting sector is mentioned as a cause of multiple critiques on the government policies. Just a small part of the hosting sector is a member of an industry organization. Hence, a central platform for the sector the communicate, exchange information, and formulating a standpoint is missing. Hence, it is difficult to get changes and new self-regulation agreements and government policies to the whole sector. Organizations can be taken by surprise and question the legitimacy of the policies. Many organizations will not commit to the agreements or implement instruments because they simply do not know they exist.

Another problem occurs on the legitimacy side of the industry representatives. The industry representatives base their standpoints on the opinions of a small part of the sector. Consequently, hosting providers do not feel represented by the industry representatives, and they are taken less seriously by the Government, as they only represent a small part of the sector. That leads to less trust in the representatives and government policies at the hosting providers. They believe the representatives have little influence and do not represent their interests. The hosting providers cancel their membership of the industry organization, will not become a member, or tries to surpass the industry representatives to lobby for their interest. Consequently, the legitimacy of the industry representatives is compromised. As a result, there is a reinforced feedback loop leading to less legitimate representation. Because hosting providers feel not represented in the policymaking of the government policies, they are reluctant to trust the quality of the policies.

A lack of trust in the government policies is reinforced by hosting providers not knowing where to go for questions, and often organizations remain unresponsive when finding them. Also, there is no platform where they ventilate their concerns because of the low organizational degree.

Communication and limited transparency lead to confusion and disappointment

Both Industry representatives and hosting providers criticized the communication of the Government. In the communication to the House of Representatives, media, and hosting providers, the Government did not recognize or openly appreciate the parties' efforts. The industry representative also noted to not recognize the public statements as being previously discussed in the PPC. Consequently, the parties said to be less well-willing to work together with the Government.

Furthermore, there were several gaps in how the hosting providers and industry representatives perceived the Government's public communication and what the Government meant. Every stakeholder makes an own interpretation. For example, the industry representatives believed that the duty of care was already decided while the Government only announced to research it. Based on the interpretation, industry representatives openly criticized the government policies and so compromising the legitimacy.

Moreover, policies established within the PPC are prompted as such. There is also little communication among the stakeholders of the PPC. Industry representatives openly communicate their concerns as they feel that the Government does not update them about their activities. Industry representatives also believe in having not enough influence on policies. An example is that after the publication of the TU Delft report, also EOKM communicated to a hosting provider that they made mistakes in gathering the data. Industry representatives immediately doubted the accuracy of the data. There was no joint solution established. The non-aligned communication decreases the trust of hosting providers in policies and instruments.

Also, the trust in the government's level of knowledge about how the Internet (sector) technically works is low. The government seems not to acknowledge the variety the sector offers. Hosting providers feel not understood and believe the government and politicians are not able to make the right trade-offs, and that there is little possibility to have a good discussion. Consequently, policies are often inadequate or infeasible. Although the Ministry of EZK recognizes that the government's knowledge level in this area can be improved, it denies that policies are not feasible or inadequate. Also, the Ministry of J&V does not share this image. The low level of trust can also be sparked by limited or confusing communication and the little contact between the hosting providers and the Government. The use of the term hosting providers is a perfect example. The Government classifies companies as hosting providers that do not classify themselves that way and are also not classified as hosting providers by law. Companies believe that the Government is unlawfully or wrongfully addressing them regarding government policies for hosting providers. However, the government policies are not only for hosting providers but do also apply to other Internet Providers, such as companies providing mere conduit services. It is a misunderstanding that the Government does not understand the difference. Nevertheless, due to a lack of communication, it seems that policies are inaccurate.

"Sometimes my company was categorized as a hoster, and then they said, "on the servers of." and "you have access to the data on the servers on your datacenter, then I needed to call again that we do not own servers and we cannot access them, and they would say "You are a datacenter, so you do have servers" –

Hosting provider

Finally, two hosting providers noted to also lack trust in studies conducted by universities or other research institutions. Data used in those studies are often inaccurate or show a too limited perspective. Conclusion are based on information provided by a small part of the "old-boys network" of the sector. Other companies are not approached or not answered if they ask question. These studies are very influential as they are often used as an important source for policymakers. Illustrative is that both hosting providers addressed that the TU Delft did perform prior checks and or seeked consultation for the TU Delft monitor report and published inaccurate findings.

NGO character of hotlines make true collaboration and intervention difficult

Competition between the hotlines exists. Although one can argue this enhances the urge to improve, it also leads to some pitfalls. As said before, a consequence is that hotlines do not want to lose their competitive advantage by sharing technologies.

Furthermore, hotlines disagree about the best procedure for the NTD mechanism and are not willing to come any closer. The Canadian hotline stepped out of INHOPE and now sends reports for the Netherlands directly to the companies instead of through the hotline. The reason for leaving was a disagreement about that INHOPE accepted funding from a company. Although INHOPE did already terminated the sponsoring contract the Canadian hotlines will not join INHOPE in a short notice as they do not agree with the current processes. The Dutch hotline reached out to the Canadian hotline to get this necessary data from them, but the Canadian hotline remained unresponsive. On the other hand, the Canadian hotline said to happily share the data with every hotline who requests them but is just unwilling to confirm the INHOPE process. This example displays the complex political environment in which the hotlines operate in which games are played and solutions are not directly sought.

Moreover, the NGO character of the hotlines also makes it difficult for the Government to interfere. The Dutch Government believes it is undesirable to try to influence NGO's as if they should remain independent. Nevertheless, the activities of the hotline directly influence the effectiveness of the government policies. The Dutch police and the Dutch hotline pointed out that with the Canadian hotline sending direct takedown requests to Dutch hosting providers, they lost sight of where CSAM is hosted and companies' take down performance. The lack of overview directly influences the completeness of the data used in the TU Delft monitor. The limited possibilities to interfere is, therefore, a risk for the accuracy of the government policies.

Risk of non-future-proof policies due to financial insecurity and political influence Besides the current pitfalls, it is also vital that the policies are ready and established for the future. The policies need to be designed in such a way that they account for any potential market or technological developments. Currently, stakeholders do not recognize a process or system dedicated to keeping up with new developments. Consequently, funding needs to be established to pay for these developments. Now the government policies and the number of resources available fluctuate at the whims of political leaders. As discussed above, in the case of Minister Grapperhaus, this had a positive outcome. Nevertheless, it can also be the other way around. The adequacy of the government policies is very dependent on their adaptation to current technologies. Consequently, nonstructural established financial resources are a risk.

7.4 Quantitative and Qualitative combined

In this section, results of the quantitative and qualitative analysis are combined to generate new insights. Where possible, the quantitative analysis is used to weigh and validate the findings of the qualitative results. Simultaneously, the qualitative results are used to give insight into the finding of the quantitative results. Only new insights created by combining the two methods are discussed below. Other insights coming forward from one of the two methods are discussed in the section above.

7.4.1 *Much unrevealed CSAM*

The EOKM, INHOPE, and IWF reports described a significant increase of reports to the Netherlands over the past years. A likely explanation for the increase is that with the implementation of proactive searching methods combined with PhotoDNA by the UK and the Canadian hotline, the findability of CSAM increased. Regardless of the increase, most stakeholders believe that just a small part of CSAM on the Dutch Internet infrastructure is found. This can clarify why the HCS already found more than 7 million images of CSAM, without PhotoDNA, and the quantity of found CSAM by the UK hotline remained the same.

The Dutch hotline processed in 2019 271.783 reports, from which 76% was illegal. The HCS found in half of the months already more than 7 million illegal images. These 7 million images are found at 54 companies that are plugged into the HCS. Not even all companies named in the TU Delft monitor report are plugged into the HCS. Hence, there is a high chance that much more content is hosted on the Dutch Internet infrastructure and not found at known and unknown companies.

7.4.2 *Unknown companies do not implement government policies*

The qualitative results showed that hosting providers base their performance on what they hear from the Government, EOKM, or industry representatives. If companies did not receive a personal call, a letter, or were named in the TU Delft monitor report, they believe there is no necessity to implement instruments like the HCS or improve their NTD processes.

There are two reasons to assume there are still several unknown companies that host CSAM. First, the top five of companies found by the Canadian hotline are different from those found by the TU Delft monitor. Secondly, not all 54 companies plugged into the HCS are named in the TU Delft monitor.

These unknown companies will not be addressed by EOKM, the Government, or the industry representatives. Consequently, it can be assumed that there are several hosting providers host CSAM and have not implemented preventive measures or fully comply with the set takedown norms.

7.4.3 *Performance measurement based on too little data*

The Canadian data revealed that many more companies do not comply with the 24-hour takedown norm in comparison to the TU Delft report. The most optimistic measurement was a compliance performance of 75% during a given period. In comparison, the TU Delft monitor measured a compliance performance of 84%. In general, one can think of two explanations: 1. On average, companies perform worse than in the sample of TU Delft or 2. Companies perform worse with notifications of the Canadian hotline instead of EOKM. Since the Canadian hotline found at least 23% of the total illegal reports of EOKM in the past, it would mean that a significant part of the found content is not deleted in the set time norm. Another explanation is that the TU Delft monitor was taken in a month, where companies performed relatively well. Both explanations show that the TU Delft report was based on not enough data to reveal companies' actual performance.

EOKM noted that SCART is not capable of accurately checking if CSAM is taken down and that due to capacity limitation, they cannot check every report manually. Additionally, the Canadian hotline wants to share its data with EOKM but skip the hotline when sending takedown requests. Consequently, EOKM is not able to monitor those reports themselves. Hence, there is a limitation in the data EOKM can gather for the TU Delft monitor to measure company performance.

Moreover, the administrative authority will issue fines based on non-compliance to the takedown orders they have sent. Therefore, is it for the authority also necessary to include the Canadian data and be capable of monitoring the real performance of companies.

7.4.4 *Limited capacity at hotlines pose risks to the adequacy of the NTD mechanism*

The quantitative results showed that EOKM processes 86% of the incoming reports within 24 hours. After 72 hours, 7% of the reports were still not processed, from which some were processed after 7000 hours. From the interview with EOKM, it can be concluded that this is caused due to capacity limitations and the level of automation of the hotline. The high number of processed reports without delay results from the automation of SCART and the adaptation of green lists. Hence, it shows the impact of automation of processes.

Furthermore, did EOKM noted that capacity is sensitive to sickness and vacations of personnel. The lack of back-up options causes high fluctuation in the number of reports that can be processed every month. This could explain the considerable variation of processed reports by EOKM. Other hotlines also noted that the availability of personnel strongly influences their quantity of processed reports. Consequently, the limited capacity of hotlines and specifically EOKM poses a risk to the adequacy of the NTD mechanism, and the effects of the government policies are challenging to see.

On the other hand, one can argue that hosters did not delete the material after receiving a notification of the HCS. It must be noted that the HCS is not implemented by all primary receivers of CSAM found by the TU Delft. This can clarify why the Canadian and the UK hotline have not seen a decrease. However, it also shows there is a lot more material on the Internet than the amount that was revealed before and handled in the NTD mechanism. Since the Ministry of J&V wants to see the total volume of found CSAM decrease, the current policies do not provide the hoped effect yet. The current system needs to be evaluated to improve the findability and takedown of CSAM.

7.4.5 *Effect of government policies are hard to measure*

The effects of the government policies on the found CSAM and companies' compliance is mainly in line with what the stakeholders concluded. The warning letters affected the adaptation of the HCS, and the quantity of CSAM found with the Instrument. Although, this had no effect on the quantity of reported CSAM by the UK. The Canadian hotline seemed to report less, but this does not necessarily have to be a result of the government policies. After the publication of the TU Delft report, the stakeholders did not observe much effect. However, the number of companies plugged into the HCS did increase a little.

7.5 Stakeholder's proposed Improvements

Sub-question 5

What are the most relevant policy improvements suggested by the stakeholders?

Categories	Examples
Improving the existing instruments	- Tailor-made norms and policies for Internet intermediates - Adding a new addendum preventive measures for hosting providers in the Code-of-Conduct
Expanding the reach of the government strategy	- Industry liaison/a personal approach to motivate hosting providers to improve their procedures - Mapping of where on the Internet CSAM is hosted
More possibilities for the enforcement of policies	- Government organisations only purchase services of companies that commit to the set norms - Increase law enforcement capacities and instruments to tackle bad/bulletproof hosters (by more providing them with more financial resources)
International expansion	- Global classification system - European adaptation of the HashCheckService
Improving participation in the policy-making process	- Closer collaboration between the sector and the government - Better organisation of the sector
Prevention and targeting demand	- More focus on prevention considering the education of parents and children - Advertising with Stop it Now! at the location of taken down material
Other	- Lawfully recognize the job of an analyst as heavy

Table 7.3: Improvement categories

The participants named 37 new unique improvements to the Government strategy. Already announced improvements are filtered out of the list. The improvements can be categorized into nine overarching areas. The whole list can be found in D. The categories and examples are displayed in table 7.5. The categories other, prevention and targeting demand, and the international expansion fall beyond this research scope as they are not an immediate improvement to the Government policy to clean the Internet of CSAM. Hence, those categories are not discussed in this section. Further, is the improvement "EOKM send a report directly to domain owner" excluded. EOKM already sends takedown requests to domain owners from which they have the abuse contact information. From the domain owners, they do not send takedown requests contact information is often not available. The more rigid check of abuse contact information by RIPE NCC is also not discussed. Hence, in none of the interviews or the literature, incorrect or non-existing abuse contact information of hosting providers seemed a problem. Below, the improvement areas and the proposed improvements are discussed.

7.5.1 *Improving the existing instruments*

During the interviews, it came forward that many stakeholders believe the idea of the instruments is, in essence, okay, but the quality is not sufficient yet. Improvements to the quality of the instruments are discussed below.

Optimizing processes of the industry

Several stakeholders believe that sharing more best practices within the sector would lead to better processes on account of the hosting providers. The qualitative results showed that many companies have different processes, sharing best practices could therefore be beneficial. Sharing best practices would contribute to the improvement of the self-regulation and support companies in adopting the most effective processes. One problem is that hosting providers are withholding in sharing all their processes for competitive considerations, and the stakeholders did not see an immediate solution to it. A second challenge is that the hosting sector is not very well organized and sharing best practices will only reach a small part of the sector. The improvement will only be useful if a large part of the sector can be reached. It is proposed to include these best practices for the NTD procedures and preventive measures into the industries CoC. Including these elements in the CoC will help companies to determine which steps they can take. Furthermore, companies believe the Government makes non-feasible policies as they do not understand the sector. Including measures in the CoC will help to increase the trust in the instruments.

Another possibility to support companies in optimizing their process is the implementation of an industry liaison. A liaison can reach out to companies to address bad performance and support them in how they can improve as the liaison has an overview of the sector's best practices. EOKM still facing staff capacity limitations, which results in little time to guide companies. Hosting providers have addressed to appreciate the collaboration with EOKM but would prefer some improvements. The qualitative results showed that companies appreciate a personal approach and believe it positively affects their performance. A personal approach is necessary to motivate companies to adopt instruments and implement procedures.

Further, an unambiguous classification of the different companies within the sector is suggested. A classification can support tailor-made procedures, policies, and norms. Self-regulation and government procedures, policies and norms are designed for the whole sector without considering the high diversity between companies. In contrast, the process description shows that hosting providers' procedures are correlated to the hosting providers' provided services. The perception of the hosting providers on the current government policies showed that the lack of differentiation and the known what is expected from them caused much frustration. With a more precise classification, tailor-made policies, procedures, and norms can be created. Consequently, companies will know better what is expected from them. Clearer expectations will lead to more adequate processes at the companies and increase the NTD mechanism's adequacy. The question is to which level of diversity the policies, procedures, and norms need to be adapted to account for the difference but not making it too complicated.

Improving the set norm

The sector brought up another improvement to the norms set by Government. Performance should only be measured with indicators the companies can influence. Several trade-offs need to be made when choosing which key performance indicators are used to measure companies' performance. During the interviews, economic and ethical arguments are brought up. Expecting compliance to a low absolute volume can, in essence, mean that some legal services will be banned from the Netherlands. Some stakeholders argue that banning services from the Netherlands compromises freedom of speech and freedom of the Internet. Banning those services could also mean that some companies will go bankrupt. Stakeholders address that when setting norms, it is essential to consider both the goal and the consequence.

Lastly, to improve the implementation and usage of instruments, one hosting provider suggested that the user-friendliness of the instruments needs to be improved. During the interviews, it was addressed that if instruments are not user-friendly, costing capacity to implement them companies will be critical before they want to use it.

However, one hoster adds that there are no reasons anymore to not implement the HCS. The hoster offers a free and user-friendly service called Qbine that scans webhosting services for CSAM using the hash database of EOKM while persevering the original webhosting environment. The hoster expects that more services will be developed in the near future.

Optimizing processes of EOKM

Several suggestions are focused on improving the processes at EOKM. The described processes in section 6.2 displayed that EOKM can still automize and improve their processes for the benefit of having fewer manual tasks. Moreover, section the missing the Canadian data poses a risk to the government policies. Also, the limited transparency about finding and processing CSAM does narrow or even distort where CSAM is hosted. To improve their processes, hotlines should share more data, best practices, and technologies with each other.

With more shared data and techniques, more processes could be automized, so less human capacity is necessary, and the system is less influenced by staff availability. However, it must be noted that it is discussed that hotlines are often not willing to share these data in the light of competitive benefits. There is no solution discussed to this. Another way is to develop those techniques for the Netherlands. However, this will not solve that the Dutch NTD mechanism is dependent on foreign hotlines' performance. Decreasing the dependency on Anglo-Saxon countries can only be done if the government policies' reach is expanded, as discussed below. Improving techniques can be done with more funding for EOKM.

Moreover, more funding to EOKM also provides the possibility to hire more personnel. Hence, this makes the processing of reports less sensitive to staff availability and give EOKM the possibility to monitor and escalate processes more often. More thorough monitoring necessary for the accuracy of the TU Delft reports.

Furthermore, the professionalization of services of EOKM is also proposed. Services include the HashCheck-Service and contact with the industry. More capacity to also focus on the contact with the industry could take away the feeling of unfairness and be wronged at the companies. The above-introduced industry liaison can also be a solution to this.

At last, it is proposed that EOKM can send monthly or annual overviews to the board of Hosting Providers about the amount of hosted CSAM on their networks. Notifying hosting provider's boards will solve some of the ignorance about the topic at the company boards. EOKM will only be able to do this if the companies provide them with the boards' contact information.

Optimizing the international NTD processes

Another discussed improvement is the international procedure of reporting to other hotlines. The Canadian hotline is convinced that It is unnecessary to send first notifications to the national hotline and let then that hotline notifies the company. Especially in the case, that material is checked with PhotoDNA because the classification is very accurate. They believe it is hindering the effective and adequate processing of notifications. "The argument that law enforcement agencies need to look at the material before takedown can take place is unrealistic. By far, most of this material is already known to law enforcement. This should not be an argument of why to delay the takedown of material" – Canadian hotline

In contrast, the other hotlines underline the importance of those steps because the national law enforcement agencies need to check if a takedown request does not frustrate any investigations.

Financing of the government policies

A source of structural financing is important for the continuity of the government policies. One Industry representative proposes a fund from which the government and industry pay all activities 50/50. Other stakeholders proposed that companies should pay for every notification they get from the Dutch hotline. The Ministry of JV believes the sector should pay for the whole approach because they profit from it.

7.5.2 *Expanding the reach of the government policies*

There can be assumed that just a small part of the CSAM on the Dutch Internet is found. Consequently, to increase the impact of the government policies, the instruments do not only have to be improved, but it is also crucial to expand their reach in terms of found CSAM.

A broader adaptation of the HCS will likely lead to finding significantly more CSAM. Companies will not act if they are not addressed by the Government, EOKM, or the industry representatives. To address all companies personally, it is vital that it is mapped where on the Internet CSAM is hosted. Mapping can be done with the use of proactive searching methods. Project LIBRA of the company WEB-IQ is created on mapping CSAM on the Internet through the dark web. It must be noted that proactive searching is forbidden by Dutch law as the Police hold a monopoly in investigation efforts. The Police and the Ministry of J&V believe that it is possible that project LIBRA does not fall under this classification. However, it needs to be closely monitored and legally checked. When being notified, those companies can also implement the HCS to screen all their services. The Industry liaison can then have a role again to assure the adaptation of the HCS.

Stakeholders addressed that there is a possibility that many companies are not aware of the existing instruments, procedures, and norms. Hence, it is proposed that another way to motivate companies to implement the HCS could be merely informing them of its existence through industry organizations. A profitable, organized sector is vital to that. The question of how to organize better the sector remains, however, unanswered.

A different proposal to motivate companies and expand the instrument's reach is to require a good performance of companies that provide service to the Dutch Government. With such a method, the Government shows to commit to the set norms and set an example to other companies. The Government's purchasing power can also have a significant financial influence on bad performing companies and, Consequently create the now missing financial incentive to some companies.

7.5.3 *More possibilities for the enforcement of policies*

Most stakeholders believe that the sector's largest share is well-willing to implement measures if they believe it is necessary. However, the Naming-and-Shaming policy's effects showed that even when companies are being made aware of their bad performance, they will not necessarily act. A way to enforce the adaptation of instruments and compliance to the set norms is vital. Additionally, an existing discontent about the current effectiveness of the law enforcement. Although the establishment of an administrative body is announced, stakeholders still believe criminal law enforcement is also necessary. A suggested measure is to significantly shorten the processing time of the criminal law enforcement procedures and execution as it is not well fitted for the digital world. Another proposed improvement is to increase the capacity and financial resources at the law enforcement agencies to tackle bad/bulletproof hosting. The latter is in line with the problem of lacking capacity at the Police, addressed by several stakeholders. More than increasing capacity, is it unclear what needs to change to make law enforcement more efficient. It is unknown how processing times at the LEA's could decrease.

Furthermore, another improvement in the category of self-regulation is the blocking of IP-addresses by Internet intermediates when other companies perform poorly. Hence, companies can choose to block all IP-addresses of non-compliant companies alone or together. When enough companies do that, including ISPs, the company is kind of blocked from the Internet. This form of self-regulation requires a definition of when companies perform poorly and requires a collaborative effort of a large share of the Internet intermediates.

7.5.4 *Improving participation and the policy-making process*

There are many critiques on the participation possibilities, collaboration, and policy-making process in general. Firstly, many parties addressed that they believe it is necessary to increase the Internet's understanding for future policymaking. One option is to improve the Government's knowledge level by hiring more specialists and pre-school civil servants. A second possibility is to have a closer collaboration between the Government and the sector. The sector can add specialized knowledge about the industry. It will also contribute to a broader support of the sector if they are more thoroughly included in the policy-making process. The sector finds influence into the policy-making process essential. Hence, it can be expected that actively including the industry will lead to high trust and more companies implementing them.

Currently, the industry representatives speak on behalf of the sector. However, the interviews sketch the expectation that many companies do not feel represented. They are not members of the industry organization or feel like the industry organization does not have enough influence. Therefore, the sector must be better organized. Again, the question of how remains unanswered. An alternative is establishing an industry liaison that could form the bridge between the sector and the policymakers.

Further, some stakeholders have called upon the Government to focus future policies on fighting bad or bulletproof hosters instead of sloppy hosters. This is in line with the sentiment that policies affecting all hosters are the fault of just a few. Further, it is also highlighted that new legal frameworks and laws need to be designed flexible for future developments.

8

Discussion, Conclusion and Recommendations

8.1 Discussion

In this section, a discussion of the results and the study methods is presented. Firstly, in section 8.1.1 the different limitations of the study are addressed. Hereafter, the choice for the mixed-method approach is reviewed in section 8.1.4. Section 8.1.3 addresses the appropriateness of the application of the theory of the rounds model of Teisman (2000). Section 8.1.5 touches upon the internal and external validity of the study. Lastly, in section 8.1.6 both scientific and practical implications of the study results are set out.

8.1.1 *Limitations*

The limitations of the study consist of limitations regarding the overall study, the qualitative analysis, and the quantitative analysis. The study's overall limitations are the fast-developing policy environment and the lack of time. The quantitative analysis limitations were the limited amount of available data and the inconsistency of the data. The limitations of the qualitative analysis include the biases of the participating hosting providers as a sector and the EC, the biases of the interviewer and interpretation errors, and intentional or unintentional inaccurate answers.

8.1.2 *Overarching limitations of this study*

A fast developing policy environment Due to the fast-developing policy environment, the results can be soon outdated. The high development pace of the Internet sector, technologies, and the timing of the study create a fast-developing environment.

The Internet sector and technologies are known for their high development pace. Technologies used by offenders and the industry are continuously changing and affecting the policies. Also, the timing of the conducted interviews contributes to the fast-developing pace of the policy environment. At the moment, The Ministry of J&V, EOKM, and the EC are continuously evolving their policies. The Dutch hotline will start to operate the HashCheckService with PhotoDNA at the end of January. The Ministry of JV starts an open consultation for the proposed administrative law in February. The European Commission has introduced the new e-privacy directive. Negotiations on the DSA are taking place, and initiatives of the European Centre against Child Sexual abuse are consulted with member states.

Furthermore, the interviews are conducted, and the quantitative data is gathered shortly after the TU Delft monitor report was published. All these developments influenced the effect of the government policies and the view of the stakeholders. Therefore, there is a risk that some conclusions in this report will be quickly outdated. For some measures, it is not possible to see a direct effect, and therefore, it is in this report too soon to jump to harsh conclusions.

lack of time During the study, the time was a serious challenge. The maximum time in which the research should be conducted was 30 weeks. Combined with a time-intensive mixed-method approach, it was necessary to set limits to the maximum amount of time spent on each element. Accordingly, some elements could not be studied (thoroughly), excluding interesting findings. For example, with more time, more explanations to the findings of the quantitative analysis could have been found and presented. Also, did some of the answers of hosting providers do not match with the RIPE WHOis database. Because of a lack of time, it was not possible to request an explanation of the hosting providers in regard to these differences.

Limitations of the quantitative analysis

Limited available data The available quantitative data is limited and messy. The organizations are not necessarily focused on gathering data and are not doing this thoroughly. Therefore, data is often inaccurate and incomplete. This has also been a limitation to this research for determining the information flows and processing times.

inconsistency of the data The data was provided by several different organizations. It was occasionally hard to determine what exactly was measured and in which unit since the organizations had limited knowledge about that. Different data sets had different levels of measurement or reflected on different time frames. Accordingly, there was inaccuracy when comparing datasets. Only mixed averages, means, medians, and high-level distributions of different time frames could be determined in the study, and several findings of different datasets could not be compared.

Limitations of the qualitative analysis

Self-selection and representability Firstly, in semi-structured interviews, there is a risk for participant biases. Also, in this research, and expected bias occurred due to self-selection and selection through recruitment via industry organizations. Hosters with bad intentions will be less likely to participate in a study in comparison with hoster with good intentions that are already involved in the policymaking of the government policies. Furthermore, hosters recruited via industry organizations are generally better informed about the policies. A couple of hosters known for regularly hosting CSAM were approached outside the original recruitment but were unwilling to participate. One hoster refused to participate because they were afraid of a backlash if they were ever identified and because of their anger towards the Dutch government for publishing the TU Delft monitor report. Three other hosters were approached but did not answer any requests.

The number of hosting providers was too low to ever reach a sufficient representation of the sector. The sector is too diverse in terms of characteristics and provided services. Also, is does the sample does not reflect the companies that are predominantly accountable for the hosting of CSAM on the Dutch Internet. Therefore, the research does not provide an all including reflection of the hosting industry. Consequently, their answers cannot be generalized to the sector.

Firstly, he interviewed hosting providers are not responsible for the largest part of the CSAM problem in the Netherlands. Since two of the six participating hosting providers were named in one of the top ten's in the TU Delft monitor report and three in the top fives extracted from the Canadian hotline's data. Consequently, this study cannot assess why these companies are getting so many more reports. The study can only make assumptions based on the thoughts of others. Secondly, there are many different types of hosting providers with different access levels to their clients' networks, with different facilities and different services. During the interviews, it became clear that these different types of providers have implemented different procedures. Consequently, sufficient representation of the different services was lacking. Finally, during the interviews, it became apparent that most participating hosting providers were relatively large companies. However, the hosting sector of the Netherlands is well known for plenty of SME-companies. Hence, it can be assumed that the sample does not reflect the Dutch hosting landscape concerning the sizes of companies.

Furthermore, the representability of the European Commission was also not completely sufficient. One employee of the Directorate-General HOME of the European Commission was interviewed. However, during the interviews, it turned out that also DG CNNCT has an essential role in the policies concerning CSAM because DG CNNCT handles the contact with the hosting sector and is responsible for the Safer Internet Initiative. It is possible that including DG CNNCT in the research could have led to relevant insight.

Inteviewer biases and response biases due to semi-structured interviews

The use of semi-structured interviews to determine processes has several limitations. The participants were often not completely aware of every process at their company or could not recall them. For example, one other hoster noted to occasionally receive notifications of EOKM but was not mentioned in the TU Delft report. Furthermore, did all hosting providers tell how many IP-addresses they operated, but this did not correspond with the RIPE WHOis database.

Also, Interviewees also tend to give more positive answers, making them look more favorable in the research outcomes (Horton et al., 2004; Hermans and Thissen, 2009). Organizations with competitive goals are not always willing to share sensitive information. Other organizations could not share all information because it is not public yet or it is sensitive information. Consequently, some data obtained about the stakeholders' processes can be incomplete or not accurate.

Furthermore, participants can be influenced by the line of questioning and the researcher's choice of words, also known as interviewer biases. To minimize biases, the researcher needs to ask non-steering open questions, which is attempted to do interview protocol. (Sekaran and Bougie, 2016). A practice interview is conducted before the first interview to establish a non-biased interview protocol. Additionally, the participants had a different background and, therefore, different levels of knowledge on the study topis. Accordingly, some participants struggled with understanding questions in specific areas. For example, some interviewees did not have heard of the HashCheckService, or of the naming-and-shaming policy of the government. In that case, the participant was provided with information. Providing interviewees with information can steer their perspective.

Perception of the interviewer

When analyzing semi-structured interviews, the interviewer interprets the answers of stakeholders. In qualitative research, there is a blurred line between objective and subjective. The study has many different layers: quantitative, process description, underlying positions, strategies, and perceptions. The combination of the high number of layers and qualitative data adds abstraction to the ground truth. During the interviews asking for underlying motivations of the participants and concluding answers was used to attempt to minimize necessary interpretations of the interviewer.

8.1.3 *Choice of the rounds model as underlying theory*

In chapter 5, it is discussed that the rounds model has some known limitations: the exact interactions and underlying motivations of decision are hard to reveal, and it is difficult to determine which factors significantly influence the policy-outcome. The underlying theory of the rounds model Teisman (2000) was used to set up the interview protocol, analyze the position of the stakeholders and the policy arena, and interpret the policymaking process. The rounds model gives a structured way to analyze the behavior of stakeholders and their relations. Often, this theory is applied to a policy evaluation. After applying the theory, it is possible to determine what kind of decisions or actions have been crucial in the policymaking process. In this thesis, the model is applied to evaluate a still ongoing policymaking process and not and not to evaluate a finalized policy. During the policymaking process, stakeholders have a larger incentive to give strategic answers. Also, without a known outcome, it is hard to validate the stated influence of participants on the policy outcome. Therefore, analyzing by means of the rounds model becomes more subjective.

Official documents are analyzed, and interviews are conducted to determine the policymaking process. Those interviews are subject to the interpretation of the researcher. Comparing how the profiles and attitudes of actors have determined the decisions and relations with other actors is subjected to the researcher's evaluation. Without the final documents showing the final results, it is hard to validate the observations.

Although the application of the rounds model of Teisman (2000) in this study has some limitations, it still represents the multi-layered and complicated policy arena and is, therefore, most suited to reveal the positions and the stakeholder's participation in the policymaking process.

8.1.4 *Choice of mixed methods approach*

As discussed in chapter 5, a well-known challenge of using a mixed-methods approach is the application of two methods simultaneously. While conducting this study, as discussed above, the limited time was a real challenge. Besides, there was limited data on this topic, and there was also little time to collect the data and analyze the data. Furthermore, the unexpected findings of this study could not all be checked or explained by executing both methods simultaneously. Therefore, some findings remain unexplained, such as why companies seem to take down more material within 24 hours than in 2019. Triangulation between the quantitative and qualitative data and results is not reached fully. Regardless of the limitations, the mixed-methods approach provided interesting insights into what stakeholders believe and what is really happening.

8.1.5 *Validation*

Internal validity

The limitation of interviewer or participant biases is already addressed. The risk of this limitation is being minimized by allowing stakeholders to withdraw at any moment, letting them indicate which answers were sensitive, and giving them the possibility to check their minutes of interviews. An open and trustworthy environment for the participants was created by providing these possibilities to the participants. Consequently, the probability of them being dishonest or incomplete has probably been reduced.

Another risk of using semi-structured interviews is that every interview progresses slightly differently than was prepared in the protocols. The data gathering on some topics, such as the pre-verification processes, are inconsistent over the virtual interviews. In some cases, the participant decided to tell more details about their process or skipped essential steps. Accordingly, it could have caused different conclusions and levels of detail within the data.

External validity

Every hosting sector per nation has specific characteristics. The Dutch industry is known for hosting many image hosters, while the German industry is more known for facilitating the financial sector. Those differences will affect the impact of certain policies and instruments. Also, the magnitude of the industry and, consequently, the volume of reports is per country very different. The workload has a significant influence on necessary actions. Optimizing and automating all processes is vital for the adequacy of the NTD mechanism and other policies in the Netherlands. In contrast, a country with only three reports per day will assumably experience more benefits than other policies. Therefore, in regard self-regulation is not limited in its external validity.

As discussed in chapter 2, different countries around the world apply other instruments for Internet governance. This study is conducted from a Western perspective, considering the Dutch and European fundamental rights. Around the world, norms such as securing and the freedom of Internet are differently interpreted and weighted. Additionally, participation in policymaking is approached differently around the world. The Dutch participation focus on this study is only relevant for countries in which participation constitutes the government type, like a participating democracy (Enserink and Koppenjan, 2007; Maleki and Hendriks, 2016; Teisman and Klijn, 2002). The external validity will therefore reach only governments with a similar point of view.

Moreover, regardless of the heterogeneity within the sector, the Internet is widespread, and companies constitute of similar systems and deal with comparable problems (Tajalizadehkhoob et al., 2016). On that level, it is possible to generalize conclusions for companies around the globe. This research is a useful step for understanding abuse and illegal content handling by hosting providers and instruments that can influence this. This research cannot yet be considered for other types of illegal content. However, hosting provider position, processes, and incentives for other types of illegal content are probable quite analogous. More research is needed to generalize this study to these types.

8.1.6 *Implications*

There are two types of implications: scientific and practical. The scientific implications describe how this research contributes to the current state-of-the-art literature. The practical implications describe how this research contributes to the government policies on cleaning the Internet of CSAM and possible broader illegal content.

Scientific implications

In section 4.5, three knowledge gaps have been identified, namely (1) the unidentified real-world execution of processes and efforts, (2) the uncertain influence of the stakeholders on policymaking, implementation, and execution, and (3)the lack of an overview of possible improvements to the system and how they can be interpreted. Based on the finding presented in chapter 6 and chapter 7, this section discusses how the research contributes to filling them.

Real-world execution of processes and efforts In the existing literature, there is little known about the real-world processes of the hosting providers and hotlines. With the use of interviews, this study aimed to map the abuse handling process within the NTD of CSAM. The qualitative results gave a more in-depth and real-life description of how CSAM is handled by hosting providers and which factors are from influence the processes. Concerning hosting providers, the results reveal different takedown systems and procedures of hosting providers concerning CSAM and general abuse. The difference in abuse handling systems is influenced by the characteristics of the hosting provider, the services they offer, if hosters are part of a re-seller construction, what type of abuse is handled, and if notifications are sent by trusted flaggers.

The services hosting providers offer influence their abuse handling processes. Regularly, companies offering mere conduit and unmanaged hosting abuse handling systems need to pass several steps to get from the intermediary who receives the report to the end-user or resource owner. Receivers are not able to directly take down the reported content without also inflicting harm to the services of many other (innocent) customers. Companies have, therefore, various possibilities to implement instruments like the NTD mechanism.

Moreover, re-seller environments reflect on the abuse handling procedures. A web-hoster that receives a takedown request has 24 hours to perform one handling to take down the content. In contrast, there are sometimes ten organizations between an infrastructure hoster and the company that can delete the content. This infrastructure hoster also has 24 hours to delete the content. Hence, their processes are very different, and other time frames are feasible. Infrastructure hosters often set a one-hour time limit to take down content to be sure to meet the 24 hours' time limit, while web-hosters follow the 24-hour norm.

Furthermore, most hosters prioritize the handling of CSAM. One hosting provider even added extra handling for CSAM notifications to take down the material faster than other forms of abuse. Some providers mentioned doing this also for other forms of abuse, like spam. Accordingly, this study showed that hosting providers prioritize categories of abuse to handle the notification quicker and that the prioritization of hosting providers is diverse. Hence, processes do also differ in that category.

Furthermore, the research of Çetin et al. (2016) finds that sender reputation does not influence the clean-up rate of hosting providers. In contrast, this study showed that all hosting providers blindly follow notifications of trusted flaggers and immediately take down the content. Sender reputation based on the classification of a trusted flagger assumable influence the clean-up rate and takedown time.

Concerning real-life processes of hotlines, it is interesting to see that there are different approaches towards finding, aggregating, checking, and notifying of CSAM. The quantitative results show that the different methods of finding CSAM have an influence on which CSAM is found.

influence of stakeholders on the (execution of) government policies The influence of relations between stakeholders on government policies is not previously studied. This research focuses on the influence of stakeholders on the Dutch system. It shows that most stakeholders are driven by moral duty and not legal obligations or financial considerations. These incentives are different from previously found financial incentives of actors in abuse handling (Jhaveri et al., 2017; Asghari et al., 2015). The found incentives show that CSAM is divergent from other forms of abuse. It is assumable that the lack of financial incentives also occurs for other forms of illegal or harmful content.

The position of stakeholders influences the policymaking and execution of government policies strongly. Hosting providers base their willingness on whether they believe it is necessary to take action. When they are not convinced policies are effective or are applicable to them, they do not implement them. Since their actions are predominantly performed from a well-willingness, hosting providers put minimal effort in keeping track of the latest developments of the government policies. Furthermore, this study observes that when trust in the government is low, proposed instruments or measures will less likely be adopted.

Moreover, the hosting sector's organizational degree influences the adaptation, trust, and participation rate of the sector. Policies and measures are scattered and not always widely supported. Government policies are also not widely spread within the sector. Self-regulation is not made in agreement with a large share of the sector, and industry representatives are often speaking on behalf of a small part of the sector. For the research field, it is challenging to generalize the opinion of hosting providers' efforts regarding CSAM and other forms of abuse.

Besides, in the field of hotlines, their positions and competitive relation reflect on the system's functioning. The competitive relation between hotlines has a direct consequence for the spread of specific technologies, data, and participation. All hotlines need to be considered as individual actors within the policy-arena. The position of hotlines directly influences their process and should therefore be kept in mind when studying those. For example, the Canadian hotline is focused solely on the well-being of children. Consequently, the Canadian hotline has no problem with sending duplicate reports to hosting providers, which believe it is annoying. While other hotlines believe cleaning the Internet of CSAM is a collaborative effort, including hosting providers, and will therefore adapt their process also to the convenience of hosting providers. The same applies to the other actors; the behavior of the stakeholders can be explained by their position. Although the objectives of the stakeholders seem quite similar when zooming into their missions and there are several conflicting objectives.

Improvements to the government policies At last, this study provides an overview of possible improvements to the government policies, section 7.5. The proposed improvements are very diverse, and it is difficult to determine the most effective policies. However, a few elements are reoccurring such as the need for a better-organized sector.

This study also shows that some government policies, such as the large scale registration of companies, can have serious implications on Internet safety, Internet freedom, economic prosperity, and freedom of speech. When establishing policies to fight CSAM other fundamental rights than the safety of a child are quickly forgotten. There is a task for the research field to consider all fundamental rights and challenge the perspectives of policymakers. In line with the research of Charalambous et al. (2016), the different fundamental rights should be considered when researching general abuse and illegal content policies.

Practical implications

In this sub-section, the practical implications of the research for the Dutch Government are discussed.

From self-regulation to co-regulation galvanizing the sector In the past years, the government strategy was based on self-regulation. The Dutch government concluded that self-regulation did not have the hoped effect. Hence, the Dutch Government is looking for more assurance and is shifting the strategy from self-regulation to co-regulation. Not only in the field of CSAM but also for cybercrime and cybersecurity policies, the sector is approached differently. The hosting industry is expected to perform better in regard to the handling of abuse. The PPC and affiliated government policies result from the new co-regulation strategy. However, the low organizational degree of the sector is a pitfall for co-regulation. The spread and implementation of policies and instruments are limited; policies are not broadly supported, and there is a limited overview of the sector.

There are no indications that the sector will organize itself better in the short term. The sector is relatively new, and it is, therefore, logical that the sector is not very well organized. However, the sector also bears a big responsibility, and it is important that it will get organized. Galvanizing the sector can have a significant impact on the adequacy and effectiveness of the government policies. Roughly two strategies can be distinguished: (1) The government chooses to regulate the sector with laws, or (2) The Government tries to enhance the organization of the sector.

Regulating the sector by law
The idea of the first strategy is that when laws are established, the sector will follow and comply with the rules. The second stage in the ladder from self-regulation to 2. co-regulation to 3. Regulation is in this option skipped. This study shows that a risk to this strategy is that many hosting providers are not aware of any government policies and will therefore not comply with new laws. Next, currently hosting providers are not always compelled to comply with the government norms as they believed it is not interesting for them or ineffective. Because the sector is not mapped, and the Dutch government does not have an overview of the sector, it is difficult to monitor and enforce government laws. Another risk is that the sector loses its willingness to do anything more than what is described in the law. There is also a risk that companies will only comply with the laws when those laws are not monitored and enforced. However, this research shows that monitoring and enforcing is rather difficult as the Dutch hosting sector is not mapped.

Enhance the organization of the sector
The idea of the second strategy is that the government actively tries to organize the sector more. However, organizing the sector is often not considered a Government task. The government should not interfere in the self-regulation and organization of a sector. Otherwise, it is not self-regulation anymore. The risk is that the government has too much influence on self-regulation, and the sector loses its own voice of belief and loses its ability to truly participate in policymaking. Nevertheless, this research identified that the government could build an own network of hosting providers, provide financial resources to the industry organizations, or support the organization with other means.

Moreover, the interviews show that many hosting providers do not feel represented by the industry organization. This study showed that because of a lack of representation, hosting providers have low trust in the government policies and are less likely to comply with them. Therefore, the government needs to strengthen and build-up a high involvement in the sector. There will only be a high involvement in the sector if the whole industry is involved, and the government is willing to cooperate truly. An extra advantage for the government is that the sector's involvement can be used to gain more specialist knowledge of how the sector works.

Another policies approach to assure adaptation of instruments and measures through the whole sector is galvanizing Internet governance bodies. They have a more extensive reach than industry organizations and have more possibilities to enforce compliance to Code-of-Conduct by, for example, blocking domains. Therefore, the government and the European Union should reach out to these companies and enhance a close collaboration. Replacing the Internet governance structure with a government structure is not necessary, but more guidance and norms should be set.

Mapping the Internet sector

Mapping the sector is necessary for monitoring and enforcing policies. In several policy fields, including CSAM but also cybercrime, mapping the Dutch hosting is a vital element. However, it is uncertain if a complete mapping of the Dutch Internet hosting infrastructure is feasible in the short-term and whether this is desirable because of two reasons. Firstly, the sector consists of many national and international companies. To map the Dutch Internet sector, all companies that operate on the Dutch network need to be registered. Secondly, an existing classification of hosting providers and Internet intermediates does not match the real-world classification. The difficulties around mapping the Internet sector makes it difficult to ensure the enforcement of policies. Policymakers identified two possibilities to map the Internet sector: (1) through a National registering system, (2) through the implementation of a duty of care.

National registering system

There are many Internet intermediates operating on the Dutch Internet infrastructure, especially due to the re-seller structure. For the CSAM policies, it is necessary to map all companies providing mere conduit or hosting services on the Dutch Internet infrastructure. That means all companies that operate have Dutch IP-addresses, and their clients, and their clients, and so on. The WHOIS database of RIPE only registers the companies operating under Dutch IP-addresses and one sub-allocate, but all other layers in a re-seller structure are invisible. It is questionable if there is an organization within the Netherlands with the capacity of mapping the whole sector. Especially since companies can be both Dutch or foreign and continuously come and go.

Duty of care

Another option is to have companies keep track of their own clients. If all companies keep track of their own clients, the government can request information when needed. Nevertheless, sometimes companies have over 100.000 clients, and one IP-address can be already used by 2000 clients. Companies with fewer personnel will struggle to comply with mapping their clients. Moreover, it is also questionable if all companies are going to comply as the government has little possibility to monitor and enforce compliance.

Desirability of registering every company

Since the Internet is a communication channel, it is uncertain whether it is desirable to register every company that operates directly or indirectly on Dutch networks. One could argue that extensive and in-depth registering interferes with fundamental rights such as privacy and freedom of the Internet. In the literature, this tension field is also pointed out (Charalambous et al., 2016).

Although both better organizing or mapping the sector does not happen overnight, organizing the sector is less controversial and is necessary to keep up with technological developments.

Enforcement of the sector

Companies need an incentive to motivate the industry to take action. The industry expresses to be well-willing and committed to doing as well as possible. However, it is evident that companies keep in mind their financial gains next to their moral duty to contribute to the government Policies. Currently, hosting providers contribute to government policies from a feeling of moral duty and to withhold themselves from reputational damage. There are no financial incentives for companies to meet the 24-hour takedown norm or implement preventive measures. During the interviews, it became apparent that most stakeholders believe an administrative authority that issues fines will solve that. In the future, it is important to create financial incentives for companies to take action. In line with this, issuing fines in the case of non-compliance can also be adopted for preventive and pro-active efforts.

Weighing feasibility, ground values, and fundamental rights when setting norms This study shows that set norms are not particularly clear for the industry. All organizations strive for their own goal; the ministry of JV, the European Commission, the Police, and the hotlines are focused on safety on the Internet. While the hosting providers, industry organizations, and the ministry of EZK are looking at a fast removal and other measures without compromising economic prosperity. The balance between economic gains and safety on the Internet should be considered when setting norms. At this point, it seems that trying to reach an absolute volume of zero reports will require the termination of all contracts with customers with user-generated content. It could also mean that other financial and economic sacrifices need to be made.

Moreover, there is a tension field between different ground values and fundamental rights. The Internet industry is also an economic sector that significantly contributes to the Dutch economy. Therefore, it should be considered very carefully if it is desirable to set norms that result in significant financial losses. Next to the necessity to consider economic consequences, it is also essential to keep in mind the role of the Internet and domains that support user-generated content. Domains are predominantly legal and function as a platform for people to share pictures and other content around the world. It can be argued that pushing these kinds of platforms outside of the Netherlands will go against the values of free communication and the Internet. All effects on fundamental rights and ground values need to be weighed very carefully.

Moreover, this study also shows that there is a risk for hotlines to be dependent on hotlines outside of the EU. Currently, the Dutch hotline and other EU hotlines do not have the capacity to collect more data to get an overview and monitor the performance of companies. Hence, the Canadian hotline leaving INHOPE had great consequences for the monitoring of the performance of companies in the Netherlands. Such data is necessary to be able to enforce compliance with the government policies.

Law enforcement of CSAM, illegal content and other forms of cyber abuse This study also reveals that stakeholders believe that the current Dutch law enforcement is not capable of sufficiently tackle CSAM online. Several stakeholders believe both bad hosters as well as downloaders and uploaders do not face any repercussion. Bad hosters can remain in business or are shut down for a few days and then re-start again. In the interviews, reasons named for this are lack of capacity, lack of knowledge, and a non-fitting system. However, some of the stakeholders have proposed improvements to law enforcement, but they all remain rather vague. Except for ramping up financial resources and capacity, there is not a directly executable solution proposed. The same problem occurs for other forms of illegal content and cyber abuse. Many states are struggling with law enforcement online. The literature also does not directly provide an answer to how law enforcement could be improved. More research is crucial to effectively improve the sector in this field.

However, it has to be noted that law enforcement alone will not be able to clean the Internet of CSAM. With preventive measures and administrative, regulatory instruments, the "bad and "good" hosters can be distinguished easier so that the police only need to investigate a smaller number of criminal offenses (Grapperhaus, 2018b).

Gap between legal classifications and real-world applications There is much literature on the classification of Internet intermediates. The European law distinguishes three types of services: (1) Mere conduit, (2)Hosting, (3) Caching. (van Hoboken et al., 2020; European Parlaiment, 2020; **?**). However, in practice, these three services lead to ambiguous real-world classification and lack to reflect all types of offered services. Consequently, it is hard to classify internet intermediates according to the legal services.

Companies often offer several services; they fall under several classifications and have different rights and responsibilities. Additionally, the CSAM government policies are based on the identification of companies through the WHOIS database. All NTD mechanisms are based on the registration of IP-addresses. Consequently, companies offering mere conduit services are often addressed and not hosting providers. Hence, Internet intermediates feel wrongfully approached, or they exclude themselves from responsibilities as they do not recognize themselves in the classification.

Approaches such as CSAM, cybercrime but also terrorist content are often focused on hosting providers. However, when sending takedown orders or requests, the IP-address operators are approached instead of the hosting providers, and these operators can also be mere conduit services. In policies, it is easily forgotten that the mere conduct services and hosting providers could both be the IP-address operators. That mere conduit services are not included in the law can lead to a problem when cleaning the Internet. Those companies will be excluded, while sometimes they are the only once's the government is able to identify.

Furthermore, the classification does not account for different services. There is still a big difference between, for example, managed and unmanaged hosting. Currently, the Ministry of Economic Affairs and Climate Policies is conducting research on the possibilities of new classifications. This will help with tailor-made policies to the possibilities of the internet intermediates and so make the policies more adequate.

Handling cyber abuse and illegal content Another practical implication is how the research reflects on handling general abuse and specifically illegal content. Hosting providers are handling CSAM and other forms of illegal content as a particular form of abuse. Therefore, trying to influence and building up a strong connection with industry governance while addressing just one kind of abuse will result in duplicating efforts. The government and the European Commission should have a more coordinated approach towards this sector.

The identified incentives moral duty and reputation damage of involved organization in the handling of CSAM is expected to be the same for illegal content. The found incentives in this research are in contrast with other previous determined incentives in the field of abuse handling. For other forms of cyber abuse, organizations often have a direct financial incentive to take action. During the interviews, several stakeholders implied that with other forms of illegal content, the incentive of moral duty is lower than with CSAM. Consequently, it means that regulating other forms of illegal content would be more problematic. Therefore, the government and other organizations with interest could better try to regulate other forms of illegal content in line with CSAM. Also, it could be beneficial to coordinate efforts, for example, similar handling of abuse and illegal, at a national or intergovernmental organization instead of all topics be handled by another team.

Influencing the European Commission Finally, the many initiatives of the European Commission will determine the path of CSAM handling in the coming years. The announced European Centre, the new legal framework, the stimulation of existing initiatives, and the enhancement of collaborations can significantly impact the Dutch and European fight against CSAM. These initiatives can solve or worsen the challenges the Netherlands is currently facing.

In recent years, the European policy concerning regulating the Internet industry was predominantly built on self-regulation of the sector (Council of Europe, 2016; Eko, 2001). Yar (2018) describes that the European Commission strategy, analogous to the Dutch strategy, is shifting from self-regulation to more co-regulation, or even ring-fenced regulation. That was confirmed by this research.

This study revealed that with the UK leaving the European Union, the UK hotline's strong influence could decrease, and there is an extra opportunity to fill their void at the EC policymaking table. This is an excellent opportunity for the Netherlands to step in and steer the EU policies. It has to be noted that the EU's policies concerning CSAM are considered separate from illegal content and general abuse.

8.2 Conclusion

This research's primary objectives were aimed at better understanding the challenges and possible improvement of the fight against CSAM in the Netherlands. The main research question was divided into five questions, which were answered in previous chapters.

Main research question

How can the Dutch government policies to clean the Internet from Child Sexual Abuse Material (CSAM) be improved?

This chapter discusses the main findings of this research and a number of future research recommendations.

8.2.1 *Key insight's*

To answer the main research question: How can the Dutch government policies to clean the Internet from Child Sexual Abuse Material (CSAM)be improved?

A mixed-method approach is applied. A quantitative data analysis is performed to reveal the information flows and processing times of the NTD mechanism and the HCS. Simultaneously, 21 semi-structured interviews with 19 different organizations are conducted. These interviews were conducted to provide insights into four elements: the detailed processes of organizations, the position, and behavior of the stakeholders in the policy-arena, how the stakeholders evaluate the current Government policies, and which improvements they propose. The theoretical basis of the rounds model of Teisman (2000) is applied to determine the position, strategy, and relations between the actors and how this influences the policy-making process.

In total 6 hosting providers, 5 hotlines (NL 2x, UK, US. Canada, and France), 3 policymakers (Ministry of JV, Ministry of EZK, and DG HOME from the European Commission), the Dutch special police force Child abuse (TBKK 2x), the community of one Internet governance body (RIPE NCC), INHOPE and 3 Industry representatives (from which one was also a hosting provider) were interviewed. The quantitative results, qualitative results, and those combined led to eight key insights to answer the research question.

The essential but unstable role of the hotlines

Hotlines have an indispensable role in the CSAM NTD mechanism (self-regulation) and the Government policies. Hotlines classify the material and send takedown requests to hosting providers. They also monitor if the material is taken down, send reminders and inform law enforcement. Additionally, for the Dutch government policies, EOKM provides the data for the TU Delft monitor.

Automatic systems and technologies like PhotoDNA help to lighten the workload. EOKM has been able to process most of the backlogs. However, the majority of the hotlines report that they struggle with lacking staff capacity. The lack of staff capacity results in backlogs of reports, the impossibility to monitor all reports, and limited guidance to the sector. EOKM is not able to monitor all reports or escalate reports if they are not taken down. The processes of the Canadian and the UK hotline showed that more automation is possible. However, hotlines have a competitive relationship, and it is unlikely that they will share all technologies with each other. Moreover, to assure a thorough process, not all steps can be replaced by automatic systems. A combination of a higher degree of automation and having enough staff capacity is necessary to ensure the adequate functioning of the NTD mechanism. If EOKM has enough capacity to escalate reports to domain registries of registrars, all content could possibly be taken offline within a certain time frame only through self-regulation. This will also lighten the workload of the police who now often need to send takedown order to companies but does not have the time to monitor the outcome of these orders.

With the establishment of the regulator of the administrative law, the relations with registries and registrars need to be determined again. It is also not unlikely that an administrative authority can work with registrars and registries to block IP-addresses and takedown domains. Furthermore, if EOKM would have enough capacity, it can also provide more data for the TU Delft monitor. The data of the Canadian hotline showed that it is assumable that companies perform worse than in the sample of the first TU Delft monitor. To get a complete oversight on the performance of companies and the possibility to act upon their bad performance, it is necessary that this data of the Canadian hotline will be included in the future.

A good collaboration between the hotlines to share data, optimize processes, share technologies and lobby for the same things will make the whole NTD mechanism and their influence more effective. Currently, the competitive character of the hotlines has a negative effect on the cleaning of the Internet. Actions to assure their competitive advantage can frustrate the adequate cleaning of the Internet. The majority of the hotlines are said to have experienced acts of other hotlines such as: not sharing data, not wanting to work along, not wanting to give in, or even frustrating the adequate execution of (government) policies/the NTD mechanism. Unfortunately, INHOPE is currently not able to bring these parties together in a sufficient manner. Hotlines outside the European Union have the possibility to step out of the INHOPE network as the Canadian hotline did. That most of the CSAM reports are originated from Anglo-Saxon countries poses a risk because of the lack of transparency and the possibility to stop sharing data with EOKM. For Dutch government policies, it is necessary that the network of hotlines will give more assurance that data will be shared and technologies will be exchanged.

The announced European center against CSA aims to establish a reliable EU wide approach. THE CSA center could possibly have a role in creating a real exchange of knowledge between hotlines and mapping CSAM on the Internet. Since the mandate and activities of the center are not yet established, it gives the Netherlands a chance to influence the outcomes. Influencing this process would require the Dutch Government to take a more proactive strategy in regard to the EC's commission strategy against CSA(M).

Low degree of organization of the sector makes self-regulation, co-regulation, and regulation difficult

The low degree of organization of the sector is a pitfall for self-regulation, co-regulation, and regulation efforts. It makes it difficult to create widely supported policies, spreading established policies, monitoring the compliance of policies, and issue sanctions when policies are violated. Furthermore, the low organizational degree does also not positively influence the sharing of best practices. Companies are also noted to not be willing to share best-practices for competitive reasons.

Only a small part of the sector is associated with the industry organizations. It is addressed that companies feel that the industry organization is kind of an "old boys" network of the hosting sector. Therefore a part of the sector does not feel represented by them. Some companies do not see the use of being a member of an industry organization and believe there is no such thing as self-regulation. Further, most of the hosting providers (members and non-members of industry organizations) believe the influence of industry representative on the government policies is too small. Accordingly, the hosting providers believe the industry representatives are not capable of representing the sector.

Moreover, for the hosting sector, it is also important to become more organized. Sharing best-practices can help the industry to optimize processes and determine what kind of instruments and policies are effective and feasible. The best examples of this are in the category of preventive measures. There are many options, and different companies have different instruments, systems, and processes. Sharing these will help them to optimize their processes and determine which processes work most adequately. Better organization will also increase their influence on government policies. With already effective and established self-regulation, the government can follow those existing practices, and this would prevent uncomfortable laws and policies from being established. With effective self-regulation and abilities to adapt to new developments, government interference would become less necessary. Industry organizations and companies need to find a way to organize themselves better. Possibly Internet governance bodies, like RIPE NCC, can support the organization of the sector because it is in their best interest too.

The implementation of government policies is very closely linked to the organization degree of the sector. The industry is relatively young but bears an enormous responsibility. Nothing indicates that in the short term, a large share of the sector will organize itself. Because of the following arguments, the government should consider intervening: Firstly, it helps if companies have the feeling that industry organization has a respectable influence on government policies. By involving and informing industry representatives more thoroughly, the government strengthens their position and increases the trust in the representatives and, therefore, also in government policies. When policies are created with the use of the specialized knowledge of the industry, the policies will benefit their efficiency and make them better. An industry liaison is another option to fill the gap of the industry organization. An industry liaison can build a broad network in the sector, gather opinions across and guide the companies in the implementation of policies. However, a downside is that an industry liaison can never take a coordinating role in self-regulation.

Necessity for an unambiguous, tailor-made and weighted classification and norms

The current classification of internet intermediates seems to categorize all companies into the same group of "hosting providers". Because companies hosting CSAM are identified by means of their IP-address, some of the companies are actually not hosting services. Those companies feel wronged. Furthermore, the research showed that the group of hosting providers is very diverse. The processes and possibilities of hosting providers are very dependent on their characteristics, like the company size, but most importantly, they depend on the services they offer. The offered services determine their level of access to the network of their clients. Within the government policies, there no distinction based on the different levels of access. Therefore, companies sometimes have the idea that the policies do not apply to them or do not know how to comply with them. Policies also have different kinds of impact on the different companies. Furthermore, in the norms set, for example, the 24-hour takedown norm, all companies are treated the same. This is problematic/inefficient/unfair because not all companies have the same capacities or possibilities needed to comply.

Furthermore, not all norms the hosting providers need to comply with are completely clear to the sector. For example, the hosting sector doubt if their performance is measured based on the takedown time or total volume, or both. There are also no set guidelines on proactive monitoring, pre-verification of clients, and other instruments. From a safety perspective, a low volume of CSAM on the Internet means better protection of children. From an economic and company perspective, it is more logical to look at the take downtime. The amount of CSAM on networks is dependent on many factors and cannot be completely influenced by hosting providers without seriously compromising their business model. An example of such a factor is providing services suitable for image hosting.

Setting norms and implementing policies can have a great influence on the economic welfare of the sector, safety on the Internet, privacy, and Internet freedom. Before setting a norm or implementing a policy, it should be considered which instruments are needed to reach such norms and which consequences it will have for the different hosting providers and Internet users. Furthermore, clear classification and communication will help to address and reach the right companies. Norms and policies adapted to the differences of companies can be established in self-regulation, especially in the field of preventive measures such as an HCS or a Know-Your-Customer policy. Companies known best which kind of measures are effective and possible per kind of company. Ideally, the government can follow those self-regulation policies and steer them in a more co-regulation strategy, in which the government also provides instruments or resources for the policies.

Much CSAM remains unfound

The enormous quantity of more than 7 million found images of CSAM by the HCS in comparison to the around 300.000 illegal reported images by EOKM in 2019, shows that with the NTD mechanism, much content remains unfound. Comparing the data of the Canadian hotline and the report of the TU Delft monitor shows that both identify different companies in their top five. Additionally, the companies plugged into the HCS services are not all named in the TU Delft reports. Consequently, it can be assumed that more CSAM is hosted at known and unknown companies on the Dutch Internet infrastructure.

A broader adaptation of the HCS will help to reveal the hosted CSAM. However, the unknown companies are not likely to implement the HCS if they are not aware of the fact that they host any CSAM. This study showed that directly and personally informing or calling out hosting providers seem to be the most effective way to let hosting providers implement instruments. To be able to inform those companies directly, they need to be identified. During the interviews, proactive searching with an automatic crawler for known CSAM is named as a solution to reveal more CSAM hosted on the Internet and possible new areas. It is crucial that not a classical crawler is used, in which only the already known areas are touched upon. Instead, a technique such as Project LIBRA can be considered.

Too little incentives to comply with the government policies

Most stakeholders are under the impression that a large share of the sector are intrinsically motivated to take their responsibility and comply with governmental and self-regulation policies. However, there is no financial or legal incentive to comply, and hosting providers will therefore always weigh moral a financial arguments. Consequently, if a hosting provider does not believe that a certain policy is effective or necessary, they will not implement it. The majority of the hosting providers believed that it is their responsibility to handle CSAM takedown requests adequately and, to a certain extent, prevent CSAM on their servers. They do not believe they are responsible for the functioning of the NTD mechanism or instruments. EOKM experienced in the past that companies did not want to change their processes if it was too much work.

Therefore, it is too optimistic to expect companies to implement all instruments solely based on their well-willingness. This study shows that enforcement options are quite limited. The announced Dutch CSAM administrative authority can be a solution. Issuing fines will create a direct financial incentive for companies to comply with the norms. A duty of care will also expectedly be introduced into the CSAM authority law. However, as discussed above, this immediately jumps to regulation and skips the options of self-regulation and co-regulation. However, it is expected that companies with bad intentions will be able to avoid the consequences of administrative laws. Therefore, and because most stakeholders believe offenders should face repercussions, it is also essential that law enforcement agencies can respond adequately.

Dutch law enforcement on CSAM

In general, the Dutch police struggles with effectively tackling offenders affiliated with online CSAM that are not directly involved in sexual child abuse. In line with that, more than half of the stakeholders question the adequacy of the law enforcement regarding CSAM. Because of the limited capacity (both financially and staff), they need to prioritize. Prioritization is always done in such a way that children are protected the most. Consequently, most downloaders and spreaders of CSAM are not even investigated. It is not that the police have too little data, as TBKK is overloaded with information.

Moreover, investigating hosting providers that possibly facilitate hosting CSAM is often deprioritized. When the police do investigate, it is often impossible to provide proof for illegal actions. Most of the investigations of bad hosters are conducted by the High-Tech Crimes team of the Dutch Police. During the interviews, it was addressed that law enforcement is not effective due to the fact that the mechanism around the application of criminal law is not capable of keeping up with current digital developments. However, academic literature and reports give little guidance on how law enforcement can be strengthened.

Lack of financial resources

For most proposed improvements, structural financial resources are necessary. The interviewed stakeholders in this study have conflicting opinions about who should pay what and why. Next to this, it is also the question if parties are able to pay and if they are going to pay. Different variations, from the option of the government paying for everything to the option that the sector pays for everything, and all variation in between, can be considered. Also, constructions with paying taxes or paying per CSAM notification of EOKM can be considered. A structural financial system needs to be established in order to assure adequate policies in the future.

General abuse and illegal content

This research shows that hosting providers handle illegal content and abuse with the same procedures and use the same systems when handling the CSAM. Some hosting providers said that they would manually check if they agree that it is illegal or not in the case of other forms of illegal content. A manual check also takes place with some other forms of abuse. CSAM is in the domain of Internet governance, is considered a unique form of abuse. These insights show that the NTD procedures and the whole approach of tackling CSAM should be connected more to policies against abuse in general. The government can seek more interdepartmental collaboration similar to the cooperation that already exists in regard to the policies on terrorist content.

8.2.2 *Future research*

In section 8.1.6 the implication of the research in the academic field was discussed. It showed a whole range of different topics that could be researched about the handling of CSAM, illegal content, and abuse in general.

Firstly, this research showed that the stakeholder's motivation in the handling of CSAM is not similar to the incentives of abuse handling described in early research. It showed that for the handling of CSAM, stakeholders are predominantly drive-by moral consciousness. For companies and organizations that have a goal of profit-making or ensuring their position, this often provokes a trade-off conflict. In the case of hosting providers, they do not see themself as responsible for the hosting of CSAM, so financial sacrifices are not easily made for handling CSAM. A comparable situation can be found in the collaboration of hotlines. They need to ensure their position and consequently do not always do what is best for the child. It is expected that for dealing with several other types of abuse, the same situation occurs, especially for illegal content. Therefore, it would be interesting to investigate if similar incentives are in place for other forms of abuse and what the effects of those incentives are on the action of stakeholders.

Secondly, the research showed that the characteristics of hosting providers influence their abuse handling procedures and systems. For future research, it is interesting to study how the characteristics correlate to the abuse handling in a representative sample. In this study, it was addressed that all hosting providers categorize CSAM as a particular type of abuse. It is interesting to research this also with a representative group of participants for the sector. Further, it would be relevant to investigate how other forms of illegal content and abuse are categorized and handled by stakeholders. Additionally, one of the characteristics that are considered is the re-seller structure in which many hosting providers operate. It is still unclear how CSAM and other forms are handled by re-sellers that are not IP-address owners and are not end-users.

Another factor that influences the handling of CSAM is the role of trusted flaggers. As discussed, many hosting providers prioritize takedown requests of trusted flaggers. How they determine if an organization is a trusted flagger differs per hosting provider. Future research could be conducted on which organizations are considered trusted flaggers and how hosting providers decide on that. A study into the real effect of trusted flagger on the takedown time and adequacy of abuse handling would also be fascinating.

The results showed that also in the area of the work of hotlines, there are many differences. It is not known which elements exactly influence the processing time and the processing procedures of hotlines. More research on this topic could provide insights into the adequate handling of illegal content. Moreover, this research also showed that the relations between the actors influence the on policy-creation, -implementation, and -execution. With the government taking more and more control in the field of Internet regulation, the relations between the government and other stakeholders will be redefined. Therefore, it is interesting to study how the connections between the stakeholders are working in regulating other forms of abuse and illegal content.

Finally, it is interesting to research the effects of different preventive instruments like an HCS or a Know-Your-Customer policy. Those instruments are often named as necessary to decrease the demand for CSAM and other forms of cybercrime as they create an extra barrier. However, little research is done in this field.

8.3 Recommendations

The ministry of JV can take several actions to improve the Government policies to clean the Internet of CSAM. The recommendations focus on enhancing the NTD mechanism, expanding the policies' reach, ensuring a higher level of compliance, and developing future policies. In this section, seven recommendations are made. Some suggestions are addressed at the government and to hotlines, the European Commission, and the industry. The recommendations are interdependent and, therefore, should be read as a whole.

8.3.1 *Establish an industry liaison*

The first recommendation is to establish an industry liaison. An industry liaison's main task is to spread and support the industry in adopting the current measures and instruments. It is seen that the reach of Government policies is not going much further than the industry organizations' constituency. An industry liaison can build up a broad network among hosting providers. That way, the industry liaison can spread the current instruments like the HCS.

Furthermore, the research showed that hosting providers miss a central point of contact at the government. They have questions but do not know where to go. Consequently, their trust in policies is lower, or they assume that policies do not apply to them. An industry liaison can function as a go-to person for companies and is able to approach companies personally. That way, an industry liaison can reach out and guide companies when their performance in the NTD mechanism or other preventive measures is not sufficient. A personal approach seemed to be most appreciated and deemed most effective by the hosting sector.

The announced administrative authority will also get a liaison role. Possibly the two above named functionalities can be added to the devised tasks of the administrative authority. The establishment of an industry liaison role at the administrative authority has the risk that different forms of illegal content and cyber abuse are approached as silos. While this research showed, they are interconnected for the activities of the hosting providers.

Another possibility is to establish an industry liaison role at the Digital Trust Centre (DTC). That has the advantage that the liaison can focus on more forms of cyber abuse and illegal content than only CSAM. However, the DTC has less overview of the policies and instruments around CSAM. Therefore, a liaison may be less effective for the Government policies to clean the Internet for CSAM. Furthermore, it is a risk that more and more organizations are getting involved in the Government policies regarding CSAM. A large volume of organizations makes it more challenging to maneuver, and communication becomes a more considerable challenge. These considerations should be weighted to decide at which institution a liaison will be established.

Proactive search of CSAM

Secondly, it is recommended to enable proactive searching in the Netherlands or Europe. The limited overview of the hosting sector makes it difficult, also for a liaison, to spread policies effectively. Furthermore, it is expected that just a small part of the CSAM online is found. The implementation of the HCS by more companies will contribute significantly to find known CSAM on the Internet. Currently, the HCS does not provide data on how much CSAM is found where on the Internet. Therefore, it does not contribute to the mapping of how much CSAM is hosted where. Furthermore, logically does the HCS only find CSAM at plugged-in companies. To motivate companies that host CSAM on the Internet to plug into the HCS, those companies need to be revealed. Proactive searching for material is essential and complementary to the HCS to map where CSAM is hosted and reveal unknown companies.

Additionally, solely depending on the Notice-and-takedown system and the public and Anglo-Saxon countries' reports will not adequately clean the Dutch network. The Netherlands and the whole European Union are dependent on Anglo-Saxon countries on which they have little influence. Accordingly, there is a lack of transparency about where and how those hotlines are searched. This lack of transparency undermines a complete and just monitoring of the Dutch Internet Infrastructure and is affiliated with risks that result from being dependent. Also, non-matching legislation poses a risk that certain illegal content in Europe is not recognized and never reported, and never taken down.

A proactive searching method to find known CSAM is vital to map CSAM transparently on the Dutch Internet infrastructure. Ideally, such a system does not only search already known specific domains or areas but can reveal unknown parts of the Internet. A project currently developed is Project LIBRA and aims to search for high-risk content by scanning the Dark web on hyperlinks to the open web. However, deployment of proactive searching is forbidden according to Dutch law. Although it is not yet determined if project LIBRA falls under the scope of this law for a large scale deployment of proactive searching, a legal investigation and possible revision need to be executed.

8.3.2 *Support the sector in enlarging the self-regulation*

The third piece of advice is to guide and strengthen the sector in its self-regulation. The strategy of the government has shifted from a focus on self-regulation to co-regulation or even regulation. However, ideally lines set-out in self-regulation are followed in co-regulation and regulation. Therefore, it is essential not to lose sight of self-regulation and make sure that government policies align with self-regulation agreements. Furthermore, effective self-regulation lowers the pressure on law enforcement and other Government institutions in the area of fighting CSAM and different forms of cyber abuse and illegal content. The low organizational degree, self-regulation adapted to classification, that prevention is not included, and the lack of monitoring in the sector are challenges that the government could address.

Firstly, the low organization degree is for self-regulation and government policies a significant pitfall. Policies are not effectively spread, compliance is hard to monitor, and just a small part of the sector is or feels represented. However, nothing indicates that in the short term, a large share of the sector will organize itself. It is also a must that the sector organization is professionalized. The government can step in to act as a catalyzer by providing (temporary) financial or other resources. Including industry representatives as an equal partner could also positively affect the organizational degree of the sector. A higher organizational degree will also make it easier for companies to share best practices and optimize their processes. The advice is to sit around the table with industry organizations and collaboratively create a plan to organize the sector in the interest of the government and in the interest of the industry. An industry liaison could have a supporting role in this.

Secondly, the sector can be motivated to address prevention, monitoring, and sanction into self-regulation. Currently, the NTD procedures are described in a Code-of-Conduct, but specific preventive measures not. Also, is the escalation path of reports if companies do not take down material can be more extensively described in the self-regulation. Going to law enforcement will have a long way, so blocking IP-addresses or domains through self-regulation will be more effective. Hence, registries and registrars must be included in the approach. Furthermore, registries can also have a role in the adaptation and spread of policies. They can require compliance to a code-of-conduct which provides for procedures around the NTD and prevention and act upon violations of their Code-of-Conduct.

Thirdly, companies believe that policies should be more specifically tailored to different types of companies, their services, and the level of access they have to the networks of the customers. It is crucial to establish a classification and such fine-grained policies first in self-regulation. The sector has the most overview about which elements are important to consider and the possibilities different companies have. The government can then follow the industry's classifications and policies. Besides, for the sector, it is also essential to establish self-regulation adapted to the different categories. That way, companies can choose an adequate classification and ensure the right interpretation of the government.

An industry liaison can support industry organizations by establishing a more extensive and widely supported self-regulation. It is not the intention to replace the function of the industry organizations with an industry liaison. A liaison forms a bridge between the government and the companies, while the industry organizations need to bring the sector together. However, an industry liaison can support those organizations in strengthening and expanding self-regulation.

8.3.3 *Communication to the sector*

The industry is vital for the government policies at every level. The sector often felt not informed well enough, and some policies came as a surprise to them. The communication hurt the relationship between the government and the industry organizations. Most of the frustrations seemed to be originated from miscommunications, misunderstanding, and the lack of a thorough participation process. It is recommended that the government will involve the sector more thoroughly in the process. Inform the industry in advance and try to find common ground before announcing policies publicly. As discussed above, it is expected that involving the sector truly will help to organize the sector better.

Moreover, in the communication to the sector, it is recommended to be precise with definitions and classifications. The government uses the term hosting providers to write about all companies while they do not all classify as such. Consequently, companies believe they are wronged, or the government makes a mistake if they are addressed in the government policies. Using a more specified classification will help to overcome this.

8.3.4 *Strengthen the processes of EOKM*

The work of EOKM Is indispensable to the NTD mechanism, the TU Delft monitor, and the HCS. They have an essential role in self-regulation and could even have a more prominent role if they had the time to monitor the takedown time more extensively and have the time to escalate reports if companies do not take them down at a given time. More processes at EOKM can be optimized to increase the available staff for other activities. The processes of the Canadian hotline showed that checking reports behind CAPTCHAS is possible. There are two ways to obtain these automatic systems. Firstly, provide financial resources to develop or buy such a system. Secondly, convince the Canadian hotline to share their technologies. The latter seems quite tricky due to the competition among hotlines.

Although automizing more processes will contribute to faster processes in which the manual tasks are minimized, manual tasks will always be necessary. Therefore, it is crucial to invest in more automation and ensure enough human capacity to do all vital jobs, like gathering data. Financial resources do not necessarily have to come from the government. Also, the sector can invest in the processes of EOKM, especially concerning the NTD mechanism and instruments directly used by companies like the HCS. However, this financial component remains a point of discussion. It is advised to re-think who needs to finance which part of the policies. Structural financial resources are necessary to clean not only the Internet of CSAM but also all other forms of illegal content and cyber abuse. The current systems are not suitable.

Although investing in techniques will have the desired outcome, it remains ineffective for hotlines to develop and invest money in systems and technologies to optimize their processes. The INHOPE network did not establish an environment where companies share all their knowledge so that another platform can be considered. The European Centre of Child Sexual Abuse (CSA) can play a role in coordinating the hotline efforts. That way, the investment of individual states in the fight against CSAM can be more effectively spend.

The Canadian hotline data is necessary for the government policies and the oversights of EOKM, and therefore the fight against CSAM. Hence, it is crucial for cleaning the Internet of CSAM that the Canadian hotline and EOKM will find a way to exchange this data with each other.

8.3.5 *Commission a study on how law enforcement can be more fitting for online crimes*

It is observed that the Dutch LEA's are struggling to address cybercrimes sufficiently. Accordingly, the trust of the sector and several other stakeholders in the LEA's handling the hosting, downloading, and spreading of CSAM is low. Multiple stakeholders doubted the effectiveness of Dutch law enforcement regarding CSAM. The police explained to struggle with the enormous streams of information due to their staffing capacity. They are forced to strictly prioritize saving children but cannot also investigate bad hosters and the largest CSAM downloaders' largest share. The investigation of bad hosters is also often done by the Team High Tech Crime of the police. Without investigating and prosecuting offenders, there is little possibility to enforce compliance with the criminal law. It is expected that companies with bad intentions will go to great lengths to bypass the laws that an effective law enforcement system is necessary.

TBKK believes that with more financial resources and more capacity, they are able to address the hosting, downloading, and spreading of CSAM adequately. However, looking at other countries, more financial resources do not directly lead to the solution. Moreover, the government's financial resources are limited. Therefore, it is vital to invest the resources smartly. Crimes on the Internet are expected to increase and further develop in the coming years (Europol, 2020). Consequently, it is crucial to create a strategy in making law enforcement agencies, both the police and the general prosecutor, being capable of sufficiently fighting inline crimes. Commissioning a study will also show the Internet sector the government's well-willingness to take on bad hosters instead of only "sloppy hosters".

8.3.6 *Develop a proactive Europe strategy and actively try to influence the initiatives of the European Commission*

The European Commission showed a great commitment to the fight against CSA(M). Some of the introduced initiatives in the strategy of July 2020 are far-reaching and can significantly influence the national approach. Other legal frameworks and policies are expected to influence cleaning the Internet from CSAM and other abuse majorly. The most prominent is the Digital Services Act (DSA), in which the rights and responsibilities of Internet companies can be revised. In the area of CSAM, the Netherlands took several policies that are stricter than in other European Countries. Establishing such procedures also on a European level contributes to the level playing field for Dutch Internet companies.

From the Dutch perspective, it is advisable to advocate that the center will have a coordinating role for the hotlines, galvanize the sector European-wide, accommodate proactive searches, and play a role in the sector's data exchange. Notable is that the center now is more focused on law enforcement efforts. The mandatory reporting requirement is similar to that of NCMEC and will focus on gathering reports the police will investigate. TBKK is already struggling with the high inflows of reports. Hence it is disputable if a bigger inflow of reports will have any effects. Further, a mandatory reporting requirement does not help to clean the Internet for CSAM. Proactive searching methods as described above and checking servers with a Hash Check will contribute to that.

In the coming year, the European Commission will negotiate and determine their announced initiatives' details and give effect to them. Specifically, the mandate, tasks, and other more practical CSA center elements are being defined. Accordingly, if the Dutch government wants to influence these processes, it should be done now. The CSA center can have an essential role in coordinating more European efforts since a waterbed effect caused by the Dutch policies is expected. The Ministry of J, in collaboration with the Ministry of EZK, can together form a policy on this topic. However, the DSA and other integral legal frameworks of policies are not only crucial for CSAM but also for all different types of cybercrime and cyber abuse and should be considered with all relevant partners.

A

Appendix A - Actor Analysis

Appendix starts at next page

Appendix A:

Actor Network Scan

Complete actor list

1. Hotline and Expert bureau CSAM/Expertisebureau Online Kindermisbruik (EOKM)
2. Dutch Ministry of Justice and Security
3. INHOPE network
4. Dutch Law Enforcement/Nederlandse politie Team Bestrijding Kinderporno & Kindersekstoerisme/Team Against CSAM and Child Sex Tourism (TBKK)
5. WEB-IQ
6. Directorate General Migration and Home affairs European Commission (DG HOME)
7. Hosting Providers with servers in the Netherlands
    a. Listed Ducth (e.g. Leaseweb, NForce)/Non-Ducth
    b. Not-listed (e.g. mijndomein)
8. Industry representatives
    a. ISPConnect
    b. DINL
    c. NLDigital
    d. DHPA
9. Non-dutch hotlines/Expert bureaus
    a. IWF (UK)
    b. Cybertip.ca (Canada)
    c. Point de contact (France)
    d. NCMEC
10. Sponsors EOKM
    a. SIDN
    b. Ziggo
    c. KPN
11. Europol
12. Interpol
13. RIPE NCC

Actors	**Strategic objectives**	**Problem specific objectives**	**Interest in problem (High-Medium-Low)**
EOKM	Preventing and fighting online CSAM and CSEM	Increasing the amount of CSAM that is taken down in the Netherlands, shorten the processing time and decreasing the mental pressure	High
INHOPE	Support the network of hotline in	Better support the national hotlines	Medium

	combating online CSAM	with a technical system so that more, easier and faster reports can be taken down. Also making guidelines analogous in the world.	
EC - DG HOME	Building an opener and safer Europe	(relatively) decreasing the hosting of CSAM on the internet on European Union servers	High
Ministry J&V	Facilitating a more just and safer society of the Netherlands	(relatively) decreasing the hosting of CSAM on the internet on Dutch servers	High
TBKK	Identifying victims and offenders of child sexual abuse	Decreasing the amount of “old” CSAM on the internet and finding more and faster “new” CSAM.	Medium/High
WEB-IQ	Making profit with online intelligence tools facilitating the fight against CSAM	Broader use of the HashCheckService and adaptation of project LIBRA	Medium/High
Non-Dutch hotlines (IWF, Cybertip.CA, Point de contact)	Preventing and fighting online CSAM and CSEM	Decreasing the processing time of reports and (relatively) finding more CSAM	Medium
Sponsors EOKM (not industry)	Sponsoring a charity for reputational considerations	EOKM preforms better by taking down more CSAM and faster	Low/Medium
Sponsors EOKM (Industry)	Facilitating an agency (EOKM) for receiving, checking and sending notifications	There is a good HashCheckService and more CSAM notifications are send faster.	Low/Medium
Europol	Support the authorities in Member States in preventing and	Decreasing the amount of “old” CSAM on the internet and finding	Low

	detecting all forms of criminality associated with the sexual exploitation of children	more and faster "new" CSAM.	
Interpol	Enable police all around the world to work together and fight CSAM	Decreasing the amount of "old" CSAM on the internet and finding more and faster "new" CSAM, and adding this in the database	Low
Hosting industry representatives			
Listed Dutch	Preventing and taking down notified CSAM faster in the light of direct reputational and moral reasons without big financial consequences	Less CSAM notifications are send and they are easy to take down	High
Listed non-Dutch	Preventing and taking down notified CSAM in the light of direct reputational and moral reasons without big financial consequences	Less CSAM notifications are send and they are easy to take down	Low/Medium
Not listed Dutch	Preventing and taking down notified CSAM in the light of direct reputational and moral reasons without big financial consequences	Less CSAM notifications are send and they are easy to take down	Medium/High
Not listed non-Dutch	Preventing and taking down notified CSAM in the light of direct reputational and moral reasons without big financial consequences	Less CSAM notifications are send and they are easy to take down	Low/Medium
Hosting industry representatives	Decreasing the amount of CSAM on the servers in the Netherlands and	Good preventive or reactive mechanism which is easy and without too much	High

	represent the interest of their members	financial investment adoptable for their members	

Actor’s resources and level of power

Actors	Important Resources	Replaceability	Power	Critical actor
EOKM	Owner of the Dutch NTD mechanism, Good reputation, Permission to check, Knowledge of CSAM, Systems for receiving and notifying reports	Low (currently) Medium (long-term)	Medium	Yes
INHOPE	Connection between hotlines, ICT systems for receiving and sending reports, knowledge of CSAM, Representing members, lobbying	Low (currently) Medium (long-term)	Low	Maybe
EC - DG HOME	Legislative authority, financial means and reputational influence	Low	High	Yes
Ministry J&V	Legislative, regulatory authority, financial means and reputational influence	Low	High	Yes
TBKK	Knowledge of CSAM processes, CSAM database owner, law enforcement, lobbying	Low	Medium	Yes
WEB-IQ	Owner of technical projects HashCheckService and project LIBRA, knowledge of online domain regarding CSAM	Low (currently) Medium (long-term)	Low	Maybe
Non-Dutch hotlines (IWF, Cybertip.CA,	Predominantly finder of CSAM reports, owner of hashdatabases and	Medium	Low	Yes (short term)

Point de contact)	technical knowledge on finding			
Sponsors EOKM (not industry)	Financial means, influence on EOKM activities	High	Low	No
Sponsors EOKM (Industry)	Financial means, influence on EOKM activities	High	Low	No
Europol	Connection between EU LEA’s, owner database CSAM hashes (EIS)	Medium	Low	No
Interpol	Connection between LEA’s, owner European database CSAM hashes (ICSE)	Medium	Low	No
Hosting industry representatives				
Listed Dutch	Server owner/renters, hosting CSAM, technical knowledge,	High	Low	Yes
Listed non-Dutch	Server owner/renters, hosting CSAM, technical knowledge,	High	Low	Yes
Not listed Dutch	Server owner/renters, hosting CSAM, technical knowledge,	High	Low	Yes

Not listed non-Dutch	Server owner/renters, hosting CSAM, technical knowledge,	High	Low	Yes
Hosting industry representatives	Lobbying power, Code of Conduct, members, reputation, knowledge	Medium	Medium	Maybe

B

Appendix B - Interview preparation

Appendix starts at next page

B.1 Appendix B.1 - Interview protocol

Interview protocol

Interview Protocol Thesis: Fighting CSAM with an NTD mechanism – Hosting providers

Part A: Generic Section

Instructions

Hello, my name is Marie Sam. Thank you for having me/coming. This interview involved two parts. The first part consists of general question which every participant gets. The second part is our role specific questions and depend on the answers you will give in the first round. The purpose is to get your perspective on the problem of online sexual child abuse material and gather insight into the working of the proactive and reactive notice-and-takedown mechanism. With the proactive NTD mechanism I mean preventive filtering by the use of a system like the HashCheckService. This service can detect CSAM on servers in order to delete it. The focus of the research is how the internet intermediate sector prevents CSAM from getting online and how to take it down. This out scope's initiatives in preventing or prosecuting offenders.

(Tape) recording instructions

As mentioned in the informed consent form I will record our interview with the goal of typing correct transcript and summarise this interview. After transcription it will be deleted.

Preamble/consent form instructions

In the run up to this interview, I have sent you an informed consent form. If you didn't have the chance to read and sign it yet, I have a printed version for you.

10 min

1. Have you received any reports of CSAM in the past?
    a. How many requests do you get per day/week/month?
    b. Do you get any reports from entities other than EOKM?
    c. Do you operate outside NL, if yes do you get any CSAM reports on those servers?
2. Does your organization have a dedicated abuse team?
3. Is your organisation member of an umbrella organisation?

Part A: Generic Questions -

1. What is the main objective/core business of your organisation/company in regard to CSAM?
2. Can you describe in the notice-and-takedown mechanism and the roles within the mechanism?
3. What is your organization role in the proactive and reactive NTD mechanism?
    a. Why do you believe this is your role?
    b. Why do you invest in this? (moral, financial, reputational considerations)

Part B: Specific Role Section

Finder

1. What are the protocols for finding CSAM?
    a. Which methods do you use?
    b. How many reports do you find per method per day?
    c. How much time does it cost approximal to find a report?

➔ If automated

    d. What is the searching protocol the algorithm uses?
    e. Does the algorithm only find old (already known) CSAM?

Aggregator

1. What are the protocols for aggregating reports?
    a. From which sources do you receive reports?
    b. What is the distribution of receiving reports per source?
    c. How much time does it cost approximal to process a received report?
    d. What are your decision criteria on which report you are going to handle first?

2. What are the protocols for further spreading the reports?
    a. To which organisation do you send reports?
    b. Do you have requirements before spreading the report further?
    c. Does it happen that it is not possible to further spread it and why?
    d. Do you keep track of the reports you send? How?

    ➔ If yes

    e. What do you do if you see they are not followed up?

Checker

1. What are the protocols for checking CSAM reports?
    a. What are your decision criteria on which report you are going to handle first?
    b. Do you use automated systems to check CSAM?
    c. If using a database which databases are affiliated to that?
    d. What are the decision criteria in flag it for sending to a law enforcement agency, another aggregator or a private party?
    e. How much time does it cost approximal to check a report?
2. How many checks do you preform per day?

Notifier

1. What are the protocols for notifying?
    a. When do you notify a report to a company?
    b. Who do you notify? (domain owners, hosting providers etc.)
    c. What are the decision criteria on which report to notify first?
    d. How much time costs it to send a notification?
    e. Do you monitor if a notification is followed with deleting? How?

➔ If monitored

    f. If they don't take down after a notification what do you do?

2. How many notifications do you send per day?

Reactive NTD mechanism (Remover)

1. What are the protocols you have in place for taking down CSAM?

    a. Do these protocols differ from the general abuse protocols you have in place?
    b. What is the maximum time you established for handling CSAM reports?
    c. What is the approximal time for taking down reports?
        i. Are you aware of the industry set norm of 24 hours?
    d. What is your handling protocol? (e.g. first in – first out, also in regard to "general" abuse)
    e. What is the difference between the CSAM handling and the general abuse handling?
    f. Do you have different protocols for different organizations? (e.g. EOKM, Police, Cybertip.ca)

➔ If (a part of) the protocol includes notifying clients:
    g. Which agreements did you establish in the contracts with clients for taking down CSAM?
    h. Do you check and how if your clients take down the URLS within a given time?
    i. What do you do if they don't? (-> if they don't respond at all what then)

➔ If any agreements
    j. What do you do if clients do not comply with those agreements? (like deleting it within 24 hours) (e.g. giving warnings or let go clients)

Proactive NTD mechanism

2. What are the protocols your organisation has in place for a proactive NTD mechanism? (HashCheckService)
    a. What is the handling time for following-up proactive reports?
    b. Which agreements did you establish in the contracts with clients for taking down CSAM?
    c. Do you check and how if your clients take down the URLS within a given time?
    d. What do you do if they don't? (-> if they don't respond at all what then)
3. If any agreements
    a. What do you do if clients do not comply with those agreements? (like deleting it within 24 hours) (e.g. giving warnings or let go clients)
4. If the received a letter of the ministry
    a. What did you change in your proactive protocols after the letter?

Part C: Current policy and effect of government interventions – 20 min

1. Are you satisfied with the current approach to tackle CSAM?
    a. Why?
    b. Do you believe the current approach is adequate?
2. Who do you believe is mainly responsible for the proactive and reactive Notice-and-Takedown of CSAM?
   Why?
3. In general, what should be improved in the NTD mechanism to fight CSAM being accessible on the Internet?
    a. What does it solve?
    b. Why do you believe that will have the most result?
    c. Is there a downside to the solution?
    d. Who is responsible for implementing this?

Ministries:

1. Was the effect of the letters similar to what you expected/wanted?
2. Was the effect of the naming-and-shaming similar to what you expected/wanted?
    a. What do you hope it will change?

European Union:

3. How do you look at the monitor as implemented in the Netherlands?
    a. Do you think this could be a good solution in the rest of Europe?
    b. Do you believe naming-and-shaming is a desirable way to motivate HPs?
    c. Are you worried about the waterbed effect, and what do you want to do about it?

Industry representative

4. What did you noticed within the industry after the letter was send?

5. What did you notice within the industry after the naming-and-shaming?
    a. Do you believe it motivated hosting providers in changing?

EOKM

6. What change did you notice after sending the letters?
    a. What actions did hosting providers took
7. What change did you notice after the naming-and-shaming letter of the minister?

Foreign tiplines

1. Do you also provide a proactive filtering system for hosting providers?
    a. How does it work?
    b. How many companies joined?
    c. How many images/URL's are taken down because of it?
2. Is there a system in which the performance of companies are made publicly in your country?
    a. How does it work?
    b. What is the effect?

Hosting providers

8. Did you receive a letter of the ministry of Justice and Security in June?

➔ If yes :

    a. Did you changed your policy or took action after receiving the letter?
        i. What did you change, or which action did you take?
        ii. Why did you change it?

➔ If named in the TU Delft monitor report

5. Have you read the report? Do you agree with the findings of the report ?
6. Did you change your policy, or do you want to take action?
        i. What did you change, or which action did you take?
        ii. Why did you do this?

Policymaking

1. On which elements of the approach do you feel your organization has influence? (elements are e.g. the regulation of the government, the self-regulation of the industry, the measures companies take, the policies of INHOPE/EOKM)
2. Which means does your organization use to influence the approach? (formal/informal)
3. Are you happy with the policy-making process of countering CSAM on the internet?
    a. Why?

Policy-makers

1. How does your organization enforce part of the approach?
    a. Which parts?
    b. What instruments does your organization have to enforce the approach?
    c. On who are you able to enforce the parts of the approach?

2. How are other stakeholders involved in the decision-making process?
    a. Does your organization have close relations with other stakeholders in this process?

B.2 Appendix B.2 - Informed consent form

Appendix starts at next page

Information letter regarding improving the fight against Child Sexual Abuse Material (CSAM) on the (Dutch) internet according to stakeholders – Delft University of Technology

Author: Marie Sam Rutten (m.s.rutten@student.tudelft.nl) based on examples of UK Data Services
Last changed: 20-07-2020

You are going to participate in an interview for the research on how to improve the fight against CSAM on the (Dutch) Internet according to stakeholder, for the Dutch ministry of Justice and Security. Through this letter you are informed about the data storage and handling of the gathered research material.

Goal of the interviews and project:
For the research interviews, with stakeholders who are closely involved in decision-making or execution of the Dutch approach against CSAM, will be conducted. These interviews are aimed at gathering the perspectives of the stakeholders on challenges, problems and possible solutions to improve the fight against CSAM on the (Dutch) internet. The evaluation of the current process and insights of the involved stakeholders will be used to create an overview of all possible improvements and their associated pro's and con's. Such an overview can be used by the Dutch ministry of Justice & Security to develop future policies.

Data storage:
The interview will be, dependent on the preference of the participant, recorded with a voice recorder or written down by hand. After completion of the thesis research voice-recording and non-anonymized data will be deleted. During the interview notes of discussed topics are made. The anonymized data will be stored on a storage space provided by the TU Delft. The anonymized data, transcripts and summaries, remains available for future research and will be stored on a research repository. If you want to limit this, please state it. All personal data will not be saved or used in this research.

Access to the data:

- Solely persons involved in the thesis project of the TU Delft or researchers under supervision of the researchers of TU Delft have access to the data gathered in this research.
- On request you have the possibility to receive the (anonymized) transcripts of your own interview and listen to the recording of the interview.
- After the project the anonymized interviews and summaries will be available on a public research repository.

Publication:

- The results and quotes of this interview can be anonymized published in (international) research publications.
- Academic publications can be received on request, if wanted you can contact: mariesamrutten@gmail.com

Please tick the appropriate boxes	**Yes**	**No**
Taking part in the study		
I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason.	□	□
I understand that taking part in the study involves a 60-minute interview. No other activities are asked of the participant	□	□
I give permission to make a voice recording of the interview, which will only be used to transcript the interview. This voice recording will be deleted directly after the transcript is finalized.		
Future use and reuse of the information by others		
I give permission that my anonymized transcripts of the interview will be archived on a public server provide to me TU Delft so it can be used for future research and learning. This also includes the use of data in academic publication through anonymized quotes or results.	□	□
I understand that I have the right to review all the documents about the information I provided before it is released to the public.	□	□

Signatures

________________________ ________________________ _________

Name of participant Signature Date

I have accurately read out the information sheet to the potential participant and, to the best of my ability, ensured that the participant understands to what they are freely consenting.

___________________________ ____________________ _________

Marie Sam Rutten Signature Date

C

Dutch NTD mechanism

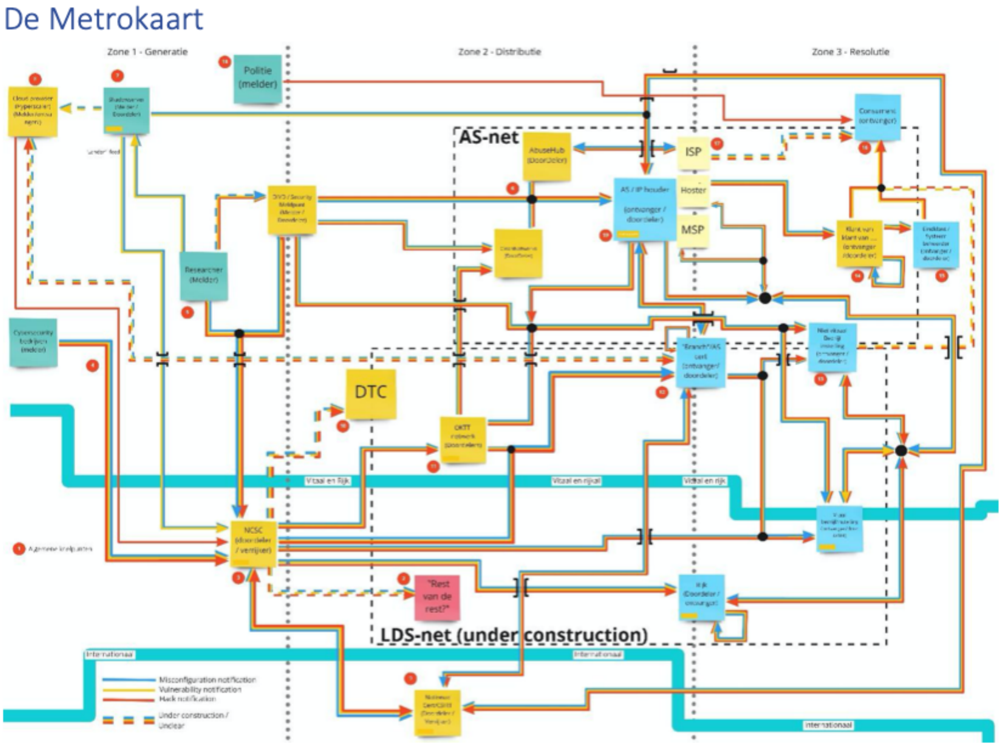
De Metrokaart
Zone 1 - Generatie
Zone 2 - Distributie
Zone 3 - Resolutie
Politie (melder)
Cloud provider (hyperscaler)
Researcher (Melder)
Cybersecurity bedrijven (melder)
AS-net
AbuseHub (Doorzetter)
ISP
Hoster
MSP
AS / IP houder (ontvanger / doordeler)
Consument (ontvanger)
Klant van klant van ... (ontvanger / doordeler)
Eindklant / Systeem beheerder (ontvanger / doordeler)
"Branch"/AS cert (ontvanger/ doordeler)
DTC
OKTT netwerk (doordelers)
NCSC (doordeler / verrijker)
"Rest van de rest?"
Rijk (Doordeler / ontvanger)
LDS-net (under construction)
Vitaal en Rijk
Vitaal en rijk/al
Vitaal en rijk
Internationaal
Algemene knelpunten
Misconfiguration notification
Vulnerability notification
Hack notification
Under construction / Unclear

Figure C.1: Metrokaart (Anti Abuse Netwerk (AAN), 2020)

The complete version can be found here `https://miro.com/app/board/o9J_lbn-wMQ=/`

D

Appendix D - Interview Results

D.1 Improvement table

Appendix starts at next page.

Improvement	Solves the problem	Suggestor
Goal: Improving the existing instruments		
The Government norm is set on the take down time instead of the volume	Companies cannot bring the volume to an absolute zero, they are dependent on many factors. Measuring the performance according to the volume on the basis of the volume can be unfair	Industry representative, majority of the hosting providers
Sharing more best practices	Within the hosting provider sector best-practices are rarely shared, that hinders the process of establishing effective procedures	Hosting providers (2x)
Tailor-made norms and policies for Internet intermediates	Measures and initiatives are focused on a group that is too big and therefore not effective. Because of this hosting providers do also feel unfairly treated and not understood.	Several hosters, industry representative (1x)
Professionalization of EOKM	The NTD procedures but also the contact with hosters is regularly unprofessional this frustrates processes and does not constitute to an adequate approach	Hosting providers (2x)
EOKM provides a monthly or annual overview for hosting providers	Boards of companies often do not know how their company is performing and do therefor not take action.	Hosting provider (1x)
Fund EOKM more to improve their processes, capacity and IT-system wise	EOKM has not enough financial resources to optimize the activities	Industry representative
More information sharing between the hotlines to improve processes	Techniques and other knowledge are not shared between the hotlines	Several hotlines
Hotlines send notifications directly to domain owners	There are too many steps between the hotline and the delete	Industry representative
Adding a new addendum preventive measures for hosting providers in the Code-of-Conduct	There are no agreements on the use of preventive measures for hosting providers and many do not use them	Industry representative

Making the instruments user-friendly (The company Severius already started the initiative and provides Qbine)	Some of the instruments, like the HCS, are not user-friendly. Hoster are discouraged by that to use it or are even not able to use it.	Several hosting providers
Industry liaison/a personal approach to motivate hosting providers to improve their procedures	The industry is immature, many companies do not succeed in getting a sufficient own abuse handling and the level of organization is very low	Industry representative, several hosting providers
Goal: Expanding the reach of the government strategy		
Web crawling or automatically searching for material by EOKM	Not enough CSAM is found and the organizations which find CSAM are not transparent about their actions	Industry representative, hosting provider (1x), EOKM, Police (only if it is old material)
Mapping of where on the Internet CSAM is hosted	Not enough material is found, and it is not clear if all non-compliant companies are addressed. Also, the police have too few leads	The ministry of J&V, Police
Industry liaison/a personal approach to motivate hosting providers to improve their procedures	The industry is immature, many companies do not succeed in getting a sufficient own abuse handling and the level of organization is very low	Industry representative, several hosting providers
Better organisation of the sector	The sector is relatively immature and has a low organization level. It is therefore difficult to communicate and the involved all relevant stakeholders in to polic-making processes	Hosting providers (2x)
Government organisations only purchase services of companies that commit to the set norms	It is hard to motivate companies to take measures because they do not understand why it is important. There are also no financial motivations	Hosting provider/industry representative
Goal: More possibilities for the enforcement of policies		
Shorten the processing time within the legal mechanism	The legal mechanism in the Netherlands take too long	The ministry of EZK

	and is therefore not suitable for the digital age	
Increase law enforcement capacities and instruments to tackle bad/bulletproof hosters (by more providing them with more financial resources)	The law enforcement does not succeed in adeqautly tackle bad hosters, that is an eyesore for the hosters and because of the impunity hosters continue with their activities and even other criminal organizations are attracted	Industry representative, Police, Majority of the hosting providers
Self-regulate blocking IP-addresses	There is little what can be done to fight bad hosters	Industry representative, Police
More rigid check of abuse contact information by RIPE	Many companies within Europe are non-responsive to abuse notification	RIPE Community
Goal: International expansion		
A better relationship between hotlines and international/foreign companies	Some regions have well fixed processes while a lot other region in the world don't. Also, the companies that are located there can and should contribute	US hotline
Global classification system	All countries apply their own classification which hinders global cleaning and law enforcement efforts	INHOPE, Dutch police
Providers around Europe scan on a larger scale their own servers	Not enough material is found	The European Commission, the Dutch police
Internationalization of the HCS	To less old CSAM is found, some companies are currently scanning but globally seen companies are not	Police
Expansion of the list of trusted flaggers internationally	Abroad there are not many organisations classified as a trusted flagger, although trusted flagger is improving the effectiveness and lowering the processing times at hosters	Hosting provider
Goal: Improving participation and the policy-making process		
The knowledge on the Internet is enriched within the government	There is lack of understanding of the Internet sector within the government	The ministry of EZK, one industry representative and multiple hosters

The policies of the government are more focussed on addressing the bad hosters	Currently, the policies of the government reach all hosters in the sector, while just a few form the problem and they can do that without any repercussions	Several hosting providers
New legal frameworks and laws are designed flexible	New laws will not be out-dated fast	INHOPE
Closer collaboration with the hotlines	Many hotlines and other similar organisations do not truly collaborate, this has a negative impact on the adequacy	Several hotlines
Closer collaboration between the sector and the government	Government policies are often not adequate and do not address the correct thing or in a correct matter	Majority of the hosting providers
Better organisation of the sector	The sector is relatively immature and has a low organization level. It is therefore difficult to communicate and the involved all relevant stakeholders in to polic-making processes	Hosting providers (2x)
Industry liaison/a personal approach to motivate hosting providers to improve their procedures	The industry is immature, many companies do not succeed in getting a sufficient own abuse handling and the level of organization is very low	Industry representative, several hosting providers
Goal: Prevention and targeting demand		
Advertising with Stop it now! at the location of take down material	There is too less attention to for preventing people from becoming an offender	Industry representative
Focus on prevention considering the education of children and parents	Children fall victim to groomers and record video; this is partly due to a poor education about safe internet use	European Commission, The Dutch hotline
Goal: Other		
Establishing more agreements to ensure employee welfare, like legally classifying it as a heavy job	The job of analyst is very heavy but not yet recognized, without the right support people can become traumatized	French hotline

The board of INHOPE will get more decisive

Bibliography

Abdullah, F. M. (2019). Crime of Extremist Content Online: Legal Challenges and Solutions. *Journal of Legal, Ethical and Regulatory Issues*, 22(5).

Açar, K. V. (2017). Organizational Aspect of the Global Fight against Online Child Sexual Abuse. *Global Policy*, 8(2):259–262.

Açar, K. V. (2020). Framework for a Single Global Repository of Child Abuse Materials. *Global Policy*, 11(1):178–190.

Adams, W. C. (2015). *Conducting Semi-Structured*.

Akdeniz, Y. (2008). Internet child pornograpgh and the law: national and international responses. chapter 9: Self-Re, pages 247–267. Ashgate Publishing Limited, Hampshire, 1 edition.

Alaerds, R., Grove, S., Besteman, S., and Bilderbeek, P. (2017). Fundament van onze digitale economie. Technical report.

Ammar, J. (2019). Cyber Gremlin: Social networking, machine learning and the global war on Al-Qaida-and IS-inspired terrorism. *International Journal of Law and Information Technology*, 27(3):238–265.

Anchayil, A. and Mattamana, A. (2010). Intermediary liability and child pornography: A comparative analysis. *Journal of International Commercial Law and Technology*, 5(1):48–57.

Anderson, J., Dodd, D., Huggins, V., Kelly, O., Knight, H., and Wickett, K. (2011). Using mixed methods: Frameworks for an integrated methodology. *Journal of Education for Teaching*, 37(4):501–503.

Angelopoulos, C. and Smet, S. (2016). Notice-and-fair-balance: how to reach a compromise between fundamental rights in European intermediary liability. *Journal of Media Law*, 8(2):266–301.

Anti Abuse Netwerk (AAN) (2020). Metrokaart en knelpunten Abuse Informatie. Technical report.

Artikel 240b SR (2020). Artikel 240b van het Wetboek van Strafrecht.

Asghari, H., Van Eeten, M. J., and Bauer, J. M. (2015). Economics of Fighting Botnets: Lessons from a Decade of Mitigation. *IEEE Security and Privacy*, 13(5):16–23.

Bae, S. M. (2017). The influence of strain factors, social control factors, self-control and computer use on adolescent cyber delinquency: Korean National Panel Study. *Children and Youth Services Review*, 78(May):74–80.

Bauer, J. M. and van Eeten, M. J. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, 33(10-11):706–719.

Bissias, G., Levine, B., Liberatore, M., Lynn, B., Moore, J., Wallach, H., and Wolak, J. (2016). Characterization of contact offenders and child exploitation material trafficking on five peer-to-peer networks. *Child Abuse and Neglect*, 52(2011):185–199.

Blok, S. (2017). Vragen van het lid Bergkamp over het bericht dat er steeds meer meldingen en materiaal van kinderporno boven water komen [Beantwoording kamervragen].

Brannen, J. and Moss, G. (2012). Critical Issues in Designing Mixed Methods Policy Research. *American Behavioral Scientist*, 56(6):789–801.

Broadhurst, R. (2019). *Child sex abuse images and exploitation materials*. Number October.

Buckley, A. P. (2015). Using Sequential Mixed Methods in Enterprise Policy Evaluation: A Pragmatic Design Choice? 13(1):16.

Calcara, G. (2013). The role of interpol and Europol in the fight against cybercrime, with particular reference to the sexual exploitation of children online and child pornography. *Masaryk University Journal of Law and Technology*, 7(1):19–33.

Carr, M. (2016). Public – private partnerships in national cyber-security strategies. 1:190–209.

Çetin, O., Hanif Jhaveri, M., Gañán, C., van Eeten, M., and Moore, T. (2016). Understanding the role of sender reputation in abuse reporting and cleanup. *Journal of Cybersecurity*, 2(1):83–98.

Charalambous, E., Kavallieros, D., Brewster, B., Leventakis, G., Koutras, N., Papalexandratos, G., and Abstract (2016). Taking stock of subjective narratives surrounding modern OSINT. In *Advanced Sciences and Technologies for Security Applications*, chapter 15: Combat, pages 57–65.

Chung, J. (2008). Comparing online activities in China and South Korea: The internet and the political regime. *Asian Survey*, 48(5):727–751.

CISCO (2020). ISP 3-Tier Model.

Coalitie AAN (2020). Child Sexual Abuse Material Dutch NTD flow. Technical report.

Cohen, M. D., March, J. G., and Olsen, J. P. (1992). A Garbage Can Model of Organizational Choice Author (s): Michael D . Cohen , James G . March and Johan P . Olsen Published by : Sage Publications , Inc . on behalf of the Johnson Graduate School of Management , Stable URL : http://www.jstor.org/stable/2. *Administrative Science Quarterly*, 17(1):1–25.

Cohen-Almagor, R. (2013). Online Child Sex Offenders: Challenges and Counter-Measures. *Howard Journal of Criminal Justice*, 52(2):190–215.

Cooper, A. (1998). Sexuality and the Internet. *Cyber Psychology & Behavior*, 1(2):813–818.

Council of Europe (2016). Blocking, Filtering and Take-down of illegal Internet content. Technical report.

Creswell, J. W. and Tashakkori, A. (2007). Differing perspectives on mixed research methods. *Journal of Mixed Research Methods*, 1(4):303–308.

Cronholm, S. and Hjalmarsson, A. (2011). Experiences from sequential use of mixed methods. *Electronic Journal of Business Research Methods*, 9(2):87–95.

Crosby, B. C. and John, M. (1992). *Leadership for the common good: Tackling public problems in a shared-power world*. John Wiley & Sons, San Fransico, 1ste edition.

Cross, C. (2018). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice*, 55(July):1–12.

Cunningham, S., Hermans, L., Reuver, M., and Timmermans, J. (2018). *Actor and Strategy model*. Hoboken.

Daucé, F., Loveluck, B., Ostromooukhova, B., and Zaytseva, A. (2019). From citizen investigators to cyber patrols: Volunteer internet regulation in Russia. *Laboratorium: Russian Review of Social Research*, 11(3):46–70.

De Bruijn, H., Ten Heuvelhof, E., and In 't Veld, R. (1998). *Procesmanagement : over procesontwerp en besluitvorming*. Schoonhaven by Academic Service, Schoonhoven.

Deibert, R. and Rohozinski, R. (2018). Control and Subversion in Russian Cyberspace. *Access Controlled*.

Demeyer, K., Lievens, E., and Dumortier, J. (2012). Blocking and removing illegal child sexual content: Analysis from a technical and legal perspective. *Policy and Internet*, 4(3-4):1–23.

DHPA (2019). State of the Dutch Data Centers 2019: Digital Awareness is Near. Technical report.

DLA Piper (2014). Legal analysis of a Single Market for the Information Society. Technical report.

ECPAT (2015). In the Shadows of the Internet Child Sexual Abuse Material in the Darknets.

Eko, L. (2001). Many Spiders, One Worldwide Web: Towards a Typology of Internet Regulation. *Communication Law and Policy*, 6(3):445–484.

Emans, B. (2004). *Interviewing, theory, techniques and training*. Stefert kroese, Leiden/Groningen.

Endeshaw, A. (2004). Internet regulation in China: The never-ending cat and mouse game. *Information and Communications Technology Law*, 13(1):41–57.

Enserink, B. and Koppenjan, J. (2007). Public participation in China: Sustainable urbanization and governance. *Management of Environmental Quality: An International Journal*, 18(4):459–474.

EOKM (2016). EOKM: Jaarverslag 2016. Technical report.

EOKM (2018). EOKM: Jaarverslag 2018. Technical report.

EOKM (2020). EOKM Jaarverslag 2019. Technical report.

EUIPO (2020). RECENT EUROPEAN CASE-LAW ON THE INFRINGEMENT AND ENFORCEMENT OF THIS MONTH ' S UPDATE ON IMPORTANT DECISIONS. Technical Report April.

European Commission (2016). EU Internet Forum: a major step forward in curbing terrorist content on the internet.

European Commission (2019). Loi visant à lutter contre les contenus haineux sur internet Emission.

European Commission (2020a). Increased amount of child sexual abuse material detected in Europe.

European Commission (2020b). Security Union: Commission welcomes political agreement on removing terrorist content online.

European Parlaiment (2020). Reform of the EU liability regime for online intermediaries. Technical Report May.

European Parliament (2020). ASSESSMENT OF PLATFORMS AND TACKLING ILLEGAL CONTENT. Technical report.

European Parliament, C. o. t. E. U. (2000). Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in theInternal Market (Directive on electronic commerce). Technical report.

Europol (2019). Internet Organised Crime Threat Assessment (IOCTA). *IOCTA report*, pages 1–63.

Europol (2020). IOCTA. *European Union Agency for Law Enforcement Cooperation 2020*.

Fishman, B. (2019). Crossroads: Counter-terrorism and the Internet. *Texas National Security Review*, 2(2):1–42.

Grapperhaus, F. (2018a). Hernieuwde aanpak online seksueel kindermisbruik [Kamerbrief].

Grapperhaus, F. (2018b). Publiek-private acties tegen online seksueel kindermisbruik en een bestuursrechtelijke aanpak [Kamerbrief].

Grapperhaus, F. (2018c). Stand van zaken aanpak Online seksueel kindermisbruik, Kindersekstoerisme en recidiverisico [Kamerbrief].

Grapperhaus, F. (2018d). Uitkomsten van de rondetafelconferentie over de aanpak van online seksueel kindermisbruik en vermeende overbelasting van de politieteams gericht op de bestrijding van kinderporno [Kamerbrief].

Grapperhaus, F. (2019a). Stand van zaken Aanpak online seksueel kindermisbruik [Kamerbrief].

Grapperhaus, F. (2019b). Voortgangsbrief aanpak Online seksueel kindermisbruik en bestuursrechtelijke handhaving [Kamerbrief].

Grapperhaus, F. (2020a). Hostingbedrijven en kinderpornografisch beeldmateriaal [Kamerbrief].

Grapperhaus, F. (2020b). Voortgang aanpak online seksueel kindermisbruik en kindersekstoerisme [Kamerbrief].

Grapperhaus, F. (2020c). Vragen van het lid Van Wijngaarden over het bericht '"Zero tolerance" is needed across Europe as figures show it's a world hub for hosting child sexual abuse material' [Beantwoording kamervragen].

Griffiths, J. (2019). *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*. Zed Books LTD, London, 1st edition.

Haans, R. (2008). *Netwerken rond e-government*. PhD thesis.

Hermans, L. M. and Thissen, W. A. (2009). Actor analysis methods and their use for public policy analysts. *European Journal of Operational Research*, 196(2):808–818.

Holt, T. J. and Bossler, A. M. (2020). *The palgrave handbook of international cybercrime and cyberdeviance*.

Holt, T. J., Cale, J., Leclerc, B., and Drew, J. (2020). Assessing the challenges affecting the investigative methods to combat online child exploitation material offenses. *Aggression and Violent Behavior*, 55(May):101464.

Horton, J., Macve, R., and Struyven, G. (2004). Qualitative Research: Experiences in Using Semi-Structured Interviews. In *The Real Life Guide to Accounting Research*, pages 339–358.

Hutchings, A., Clayton, R., and Anderson, R. (2016). Taking down websites to prevent crime. *eCrime Researchers Summit, eCrime*, pages 102–111.

ICMEC (2018). Child sexual abuse material: Model legislation & global review. page 68.

INHOPE (2018). Annual Report 2018/2019. Technical report.

INHOPE (2020a). A Deep Dive into the INHOPE hotlines' Notice and Takedown procedures. Technical report.

INHOPE (2020b). History of INHOPE.

Internation Watch Foundation (2020). IWF 2019 Annual Report | Zero Tolerance. Technical report, London.

International Centre for Missing & Exploited Children (2017). Online Grooming of Children for Sexual Purposes : Model Legislation & Global Review. Technical Report 67.

IXPDB (2020). The IXP Database.

Jacobs, D. (1993). Het structurisme als synthese van handelings en systeemtheorie? *Tijdschrift voor Sociologie*, 14(3):335–360.

Jhaveri, M. H., Cetin, O., Gañán, C., Moore, T., and Van Eeten, M. (2017). Abuse reporting and the fight against cybercrime. *ACM Computing Surveys*, 49(4):1–27.

Jick, T. D. (1979). Mixing Qualitative and Quantitative Methods: Triangulation in Action. Technical Report 4.

Jørgensen, R. F. and Zuleta, L. (2020). Private Governance of Freedom of Expression on Social Media Platforms EU content regulation through the lens of human rights standards. *Nordicom Review*, 41(1):51–67.

Kallio, H., Pietilä, A. M., Johnson, M., and Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, 72(12):2954–2965.

Kaur, H. and Tao, X. (2014). *ICTs and the Millennium Development Goals*.

Keen, C., Kramer, R., and France, A. (2020). The pornographic state: the changing nature of state regulation in addressing illegal and harmful online content. *Media, Culture and Society*.

King, G., Keohane, R., and Sidney, V. (1995). Review : Qualitative Divide in Political Science. *The American Political Science Review*, 89(2):471–474.

King, G., Pan, J., and Roberts, M. E. (2014). Reverse-engineering censorship in China: Randomized experimentation and participant observation. *Science*, 345(6199).

Kingdon, J. W. (1984). *Agendas, Alternatives and Public Policies*. HarperCollins College Publisher, New York, 1ste edition.

Kokolaki, E., Daskalaki, E., Psaroudaki, K., Christodoulaki, M., and Fragopoulou, P. (2020). Investigating the dynamics of illegal online activity: The power of reporting, dark web, and related legislation. *Computer Law and Security Review*, 38:105440.

Lacharite, J. (2002). Electronic decentralisation in China: A critical analysis of Internet filtering policies in the People's Republic of China. *Australian Journal of Political Science*, 37(2):333–346.

Lev-aretz, Y. (2014). Combating Trademark Infringement Online : Secondary Liability v . Partnering Facility. *The Columbia Journal of Law & The Arts*, 37(4):639–647.

Limoncelli, T. A., H. C. J. &. C. S. R. (2016). *The Practice of System and Network Administration: Volume 1: DevOps and other Best Practices for Enterprise IT*. Addison-Wesley Professional.

Liong, V. E., Lu, J., Tan, Y. P., and Zhou, J. (2017). Deep Video Hashing. *IEEE Transactions on Multimedia*, 19(6):1209–1219.

Lodder, A., Schimmel, M., and van den Winkerl, Y. (2016). Hoofdstuk 6 Aansprakelijkheid internet providers. Technical report.

Lone, Q., Gañán, C. H., and Eeten, M. V. (2020). CSAM Hosting Monitor Report September 2020. Technical report.

MacKinnon, R. (2009). China's Censorship 2.0: How Companies Censor Bloggers. *First Monday*, 14(2).

Maleki, A. and Hendriks, F. (2016). Contestation and participation: Operationalizing and mapping democratic models for 80 electoral democracies, 1990-2009. *Acta Politica*, 51(2):237–272.

McIntyre, T. J. (2013). Child abuse images and cleanfeeds: Assessing internet blocking systems. *Research Handbook on Governance of the Internet*, pages 277–308.

Miles, M. B. and Huberman, A. M. (2014). an Expanded Sourcebook Qualitative Data Analysis.

Mirchandani, M. (2020). *Tackling insurgent ideologies om a pandemic world*, volume 1. Observer Research Foundation, New Delhi.

Mitsilegas, V. (2021). Counterterrorism and the rule of law in an evolving European Union: Plus Ça Change ? *New Journal of European Criminal Law*, page 203228442097178.

Moore, T. and Clayton, R. (2009a). Managing Information Risk and the Economics of Security. *Managing Information Risk and the Economics of Security*, (May 2009):0–24.

Moore, T. and Clayton, R. (2009b). The Impact of Incentives on Notice and Take-down. *Managing Information Risk and the Economics of Security*, (June):199–223.

Morgan, D. L. (2017). Mixed methods research. *The Cambridge Handbook of Sociology*, 1:153–161.

Mouron, P. (2020). Son inaction en la matière lui a valu une nouvelle assignation devant le Tribuna l judiciaire de Paris par plusieurs associations, notamment l'UEJF et SOS-Racisme, en mai dernier. *Revue européenne des médias et du numérique*, 55:17–22.

Mthembu, M. A. (2012). High road in regulating online child pornography in South Africa. *Computer Law and Security Review*, 28(4):438–444.

Noroozian, A., Koenders, J., Van Veldhuizen, E., Ganan, C. H., Alrwais, S., McCoy, D., and Van Eeten, M. (2019). Platforms in everything: Analyzing ground-truth data on the anatomy and economics of bullet-proof hosting. *Proceedings of the 28th USENIX Security Symposium*, (2):1341–1356.

Norton, W. B. (2008). The Art of Peering: the Peering Playbook.

Noticeandtakedown.nl (2018a). Gedragscode Notice-and-Take-Down 2018 inclusief addendum 1.

Noticeandtakedown.nl (2018b). NTD Flowcharts.

Ognyanova, K. (2014). Careful What You Say: Media Control in Putin's Russia – Implications for Online Content. *International Journal of E-Politics*, 1(2):1–15.

Oosten, F. v. and Buitenweg (2018). Naming and shaming bij niet verwijderen van kinderpornografie [Motie].

Opstelten, I. (2013). Voortgangsrapportage kinderpornografie en kidnersekstoerisme.

Pan, J. and Zhang, T. (2019). How Companies Perpetuate and Resist Chinese Government Censorship.

Pollicino, O. and Soldatov, O. (2018). Striking the Balance between Human Rights Online and State Security Concerns: The Russian Way in a Comparative Context. *German Law Journal*, 19(1):85–112.

Ramešová, K. (2020). Public provocation to commit a terrorist offence: Balancing between the liberties and the security. *Masaryk University Journal of Law and Technology*, 14(1):123–147.

Schillemans, T. (2013). Moving Beyond The Clash of Interests: On stewardship theory and the relationships between central government departments and public agencies. *Public Management Review*, 15(4):541–562.

Sekaran, U. and Bougie, R. (2016). *Research methods for business: A skill building approach*. John Wiley & Sons Ltd., West Sussex, 1st edition.

Steel, C. M. (2009). Child pornography in peer-to-peer networks. *Child Abuse and Neglect*, 33(8):560–568.

Steel, C. M., Newman, E., O'Rourke, S., and Quayle, E. (2020). An integrative review of historical technology and countermeasure usage trends in online child sexual exploitation material offenders. *Forensic Science International: Digital Investigation*, 33:300971.

Steur, J., Vorst, T. V. D., Wijk, A. V., Driesse, M., and Sahebali, W. (2019). Mogelijkheden voor het aanpakken van kinderporno op basis van bestuursrechtelijke handhaving. Technical Report april.

Tajalizadehkhoob, S., Böhme, R., Gañán, C., Korczyński, M., and Van Eeten, M. (2018). Rotten apples or bad harvest? What we are measuring when we are measuring abuse. *ACM Transactions on Internet Technology*, 18(4).

Tajalizadehkhoob, S., Goethem, T. V., Korczyñski, M., Noroozian, A., Böhme, R., Moore, T., Joosen, W., and Eeten, M. V. (2017). Herding vulnerable cats: A statistical approach to disentangle joint responsibility for web security in shared hosting. *Proceedings of the ACM Conference on Computer and Communications Security*, pages 553–567.

Tajalizadehkhoob, S., Korczyński, M., Noroozian, A., Gañán, C., and Van Eeten, M. (2016). Apples, oranges and hosting providers: Heterogeneity and security in the hosting market. *Proceedings of the NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, (July 2018):289–297.

Teisman, G. (1992). *Complexe besluitvorming : een pluricentrisch perspectief op besluitvorming over ruimtelijke investeringen*. VUGA, The Hague, 2nd edition.

Teisman, G., van Buuren, A., and Gerrits, L. (2009). *Managing Complex Governance Systems*. Routledge, New York.

Teisman, G. R. (2000). Model for research intor decion-making processes; on phases, streams and decision-making rounds. 78(4):937–956.

Teisman, G. R. and Klijn, E. H. (2002). Partnership arrangements: Governmental rhetoric or governance scheme? *Public Administration Review*, 62(2):197–205.

Truyens, M. and Van Eecke, P. (2016). Liability of domain name registries: Don't shoot the messenger. *Computer Law and Security Review*, 32(2):327–344.

Tweede Kamer (2018). Tweede Kamer, 65e vergadering [Plenaire Vergadering].

van Eeten, M., Lone, Q., Moura, G., Asghari, H., and Korczyński, M. (2016). Evaluating the Impact of AbuseHUB on Botnet Mitigation.

van Hoboken, J., Appelman, N., van Duin, A., Blom, T., Zarouali, B., Ó Fathaigh, R., Seel, M., Stringhi, E., and Helberger, N. (2020). WODC-onderzoek : Voorziening voor verzoeken tot snelle verwijdering van onrechtmatige online content. Technical Report september, Universiteit van Amsterdam.

Van Hoboken, J., Quintais, J. P., Poort, J., and Eijk, N. v. (2018). Hosting Intermediary Services And Illegal Content Online: An analysis of the scope of article 14 ECD in light of developments in the online service landscape. Technical report.

Von Behr, I., Reding, A., Edwards, C., and Gribbon, L. (2013). Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism. Technical report, Cambridge.

Wang, J. (2018). Regulating Hosting ISPs' Responsibilities for Copyright Infringement. *Regulating Hosting ISPs' Responsibilities for Copyright Infringement*, (2016).

Web-IQ (2018). Web-IQ newsletter. Amsterdam: Web-IQ.

Web-IQ (2020). Corona report #1 Confidential. Technical report.

Westlake, B., Bouchard, M., and Frank, R. (2017). Assessing the Validity of Automated Webcrawlers as Data Collection Tools to Investigate Online Child Sexual Exploitation. *Sexual Abuse: Journal of Research and Treatment*, 29(7):685–708.

Westlake, B. G. and Bouchard, M. (2016). Liking and hyperlinking: Community detection in online child sexual exploitation networks. *Social Science Research*, 59:23–36.

Wijk, A. V., Dickie, S., and Ham, T. V. (2019). Downloaders van kinderporno ; een literatuuronderzoek. Technical report.

Wilms, P. (2012). Evaluatie doelmatigheid Fraudehelpdesk.

Wilson, C. (2014). *Interview techniques for UX practitioners*. Elsevier, Waltham, 1ste edition.

Yar, M. (2018). A Failure to Regulate? The Demands and Dilemmas of Tackling Illegal Content and Behaviour on Social Media. *International Journal of Cybersecurity Intelligence and Cybercrime*, 1(1):5–20.

Zulkarnine, A. T., Frank, R., Monk, B., Mitchell, J., and Davies, G. (2016). Surfacing collaborated networks in dark web to find illicit and criminal content. *IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data, ISI 2016*, pages 109–114.

TU Delft