ENFORCING THE LAW IN CYBERSPACE

Exploring cyber enforcement capabilities for the police in the Netherlands

MSc. in Policing
Master thesis
H.B. Aalbers MSc.
221576

Canterbury Christ Church University

POLITIE
Politieacademie

Abstract

Little research has been done on active and openly performed police law enforcement in cyberspace. In this explorative study, the possibilities and constraints for police to use cyber enforcement methods were analyzed. A theoretical analysis shows that the police authority to use legitimate force is also applicable to cyberspace. In-depth interviews with 14 experts on various relevant disciplines were conducted to compose a list of the following potential enforcement methods: high layer (D)DoS attack, UMTS/WiFi Internet shutdown, hack, and criminal data distortion. Article 3 from Dutch Police Law probably provides an adequate legal basis to use some methods, whereas others need law amendments, according to the legality principle. It depends on whether or not the method causes more than a minor infringement of the basic rights of the person. Further research could provide clarity about the effectiveness of these methods and about the legal challenges when used against targets in other jurisdictions.

"Research is to see what everybody else has seen, and to think what nobody else has thought."
Albert Szent-Gyorgyi (1893 – 1986) Physiologist and Nobel Prize recipient

CONTENTS

INTRODUCTION: EXPLORING CYBER ENFORCEMENT CAPABILITIES FOR THE POLICE IN THE NETHERLANDS 5
RESEARCH QUESTIONS & RESEARCH DESIGN 6

1. THE POLICE TASK AND THE AUTHORITY TO USE LEGITIMATE FORCE 7
1.1 PRESENT AND PAST 7
1.2 CURRENT USE AND INSTRUCTION ON THE USE OF FORCE (*"GEWELDSINSTRUCTIE"*) AND THE ABSENCE OF OFFENSIVE CYBER CAPABILITIES 9
1.3 PRE-CONCLUSION 9

2. CYBERSPACE AND THE DIFFICULTIES OF CRIMINAL INVESTIGATION 11
2.1 THE OMNIPRESENCE AND IMPORTANCE OF CYBERSPACE 11
2.2 TWO CRIMINAL PHENOMENA IN CYBERSPACE AND THE DIFFICULTIES OF INVESTIGATION 14
2.2.1 (D)DoS attacks and Illegal trade on TOR hidden services 14
2.2.2 Survey: difficulties of investigating (D)DoS and illegal trade on TOR hidden services 16
2.3 THE DISRUPTION ALTERNATIVE 18
2.4 PRE-CONCLUSION 19

3. THE AUTHORITY TO USE LEGITIMATE FORCE IN CYBERSPACE 20
3.1 TRANSLATING THE POLICE AUTHORITY TO USE FORCE TO CYBERSPACE 20
3.2 PRE-CONCLUSION 22

4. POSSIBILITIES AND CONSTRAINTS OF LAW ENFORCEMENT IN CYBERSPACE, SEEN FROM A LEGAL, ETHICAL AND SOCIETAL PERSPECTIVE 23
4.1 LEGAL PERSPECTIVE 23
4.2 ETHICAL AND SOCIETAL PERSPECTIVE 28
4.3 PRE-CONCLUSION 30

5. POTENTIAL ENFORCEMENT METHODS IN CYBERSPACE 32
5.1 HOW AND WHEN TO USE: PROPORTIONALITY, SUBSIDIARITY AND OTHER CONSIDERATIONS 32
5.2 POTENTIAL ENFORCEMENT METHODS IN CYBERSPACE AND CHARACTERISTICS 34
5.2.1 (D)DoS attack 35
5.2.2 Internet shutdown 38
5.2.3 Hack & shutdown/encrypt/destroy 39
5.2.4 Criminal data distortion 42
5.2.5 Discarded methods 43
5.3 COMPARISON OF THE POTENTIAL ENFORCEMENT METHODS 46
5.4 PRE-CONCLUSION 47

6. DISCUSSION 48

7. CONCLUSIONS AND RECOMMENDATIONS 49
7.1 CONCLUSIONS 49
7.2 RECOMMENDATIONS 50

REFERENCES 52

CASE LAW AND PARLIAMENTARY DOCUMENTS 57

Introduction: exploring cyber enforcement capabilities for the police in the Netherlands

The time of cyberspace as something separated from the physical world is long gone. More and more, the physical and virtual worlds are intertwined: cyber events have an impact on the physical world, and the other way around. Perhaps one of the most striking examples is the Stuxnet worm, a piece of computer software that broke into an Iranian uranium enrichment facility. It successfully infected a number of uranium centrifuges and, allegedly, temporary disrupted operations (Farwell & Rohinski, 2011). But the impact is also seen in totally different ways: how about the on-line thermostat application which enables you to warm up your home from far away (Baraniuk, 2014), or the car navigation system with real time traffic monitoring, which brings you home more quickly (Cohn, 2012).

The number of devices connected to the Internet is growing very fast and experts predict the evolution from an Internet of Things (IoT) to an Internet of Everything (IoE) (Evans, 2012).

While legislation and criminal investigation both take more shape in cyberspace, active enforcement of (cyber) law and emergency assistance by the police seem to lag behind. Most police activities in cyberspace are secretive. This could have to do with a fear among citizens and politicians, to create a so called "surveillance state", whereby openly and active police presence on the Internet can be interpreted as privacy intrusion. But which is more privacy infringing in the end: a transparent police with a number of enforcement methods that are publicly announced when used, or a police who secretively use investigative powers?

The more discrete method: criminal investigation in cyberspace, becomes a mission impossible in some cases, caused by suspects tucked far away abroad, behind encryption, anonymous TOR networks and bullet proof hosting providers (McCoy, Bauer, Grunwald, Kohno & Sicker, 2008; Krebs, 2010). This is a problem for the police: one of their main tasks is the effective enforcement of the law.

A possible alternative to investigation and prosecution of criminals is disrupting and obstructing them: looking for ways to disturb criminal business processes. The strategy of disruption is already widely used by the Dutch Police, the thoughts behind it were introduced around 2003, in a report called "Obstruction as Asset" (originally "Tegenhouden Troef", in Dutch)(Projectgroep Opsporing-2, 2003). However, disruption is not frequently seen in cyberspace yet.

Possibly, in the near future, choosing the attack and deploying cyber enforcement methods could offer interesting possibilities for the police. In the physical world the police have the possibility to use force, and a number of weapons and tactical units to scale up and down when appropriate. But how does this work online? The current instructions for the use of force are solely focused on physical force and not on 'cyber' force whatsoever (Ministerie van Justitie, 1994). Can we determine enforcement capabilities in cyberspace, and when should they be deployed? The objective of this master thesis is to examine whether the definition of "police force" can be applied to cyberspace, and what cyber enforcement capabilities would look like.

This research contributes to both academic knowledge base as well as police practice. There is very little research that makes a comparison between police use of force in the physical world and cyberspace, so this thesis opens up the path for other authors to start thinking, writing and conducting empirical research about the theme. Furthermore it can help police organizations in the Netherlands and abroad that are struggling with cybercrime to start defining and exploring their offensive capabilities in cyberspace.

Research questions & research design

Main research question:

How can the police authority to use legitimate force in the Netherlands be translated to cyberspace, what are potential enforcement methods in cyberspace, and what possibilities and constraints do they entail from a legal, ethical and societal point of view?

The main research question has been subdivided into eight sub-questions:

1. What does the police authority to use legitimate force entail and does it encompass cyberspace? (see section 1.1 & 1.2)
2. What is 'cyberspace', what role does it play in contemporary society and should the police carry out their task in cyberspace? (see section 2.1)
3. What difficulties arise when the police are conducting criminal investigations in cyberspace? (See section 2.2)
4. What is the strategy of disruption and is it an interesting alternative to tackle cybercrime? (see section 2.3)
5. Is the police authority to use legitimate force also applicable to cyberspace? (see section 3.1)
6. What are the possibilities and constraints of enforcement in cyberspace, seen from a legal, ethical and societal point of view? (see sections 4.1, 4.2 & 4.3)
7. When and how should the police use these enforcement methods, also considering the principles of subsidiarity and proportionality? (see section 5.1)
8. What are potential enforcement methods in cyberspace, and what are their characteristics? (see sections 5.2 & 5.3)

Research design

This master thesis consists of several sections in which different research methods are used.

The first chapters, 1, 2 and 3, form the theoretical basis of this thesis. Those chapters consist of a literature study into the police use of force and cyberspace. In paragraph 2.2.2, findings from literature are supplemented by empirical findings: a survey conducted amongst employees from the Dutch National High Tech Crime Unit. They were asked by e-mail to fill out the survey about the difficulties of investigations in cyberspace. Response was also by e-mail to make it as easy as possible for the employees to take part, to get a good response rate. The survey gives valuable insights on the problems that investigators run into when they conduct investigations in cyberspace.

It is only meant as a supplement: semi structured expert interviews form the empirical backbone of this thesis. Fourteen experts were selected to conduct in-depth interviews, in which the technique of active listening was used (Guion, Diehl & McDonald, 2001). Especially paraphrasing what the speaker said and reflecting it was extensively done to derive the most complete answers. Before each interview, a set of open-ended questions was prepared, mostly resembling the research questions. To create a multi-perspective research, a diverse list of respondents was created. Experts from public and private organizations, with backgrounds in technology, law, ethics, cybercrime and cyber security were interviewed. The interviews were recorded and fully transcribed. After analysis, the coded interview fragments were used as input for chapters 4 and 5.

1. The police task and the authority to use legitimate force

1.1 Present and past

In Dutch Police law, article 3 describes the task of the police as: *"carrying out the effective enforcement of law and order and providing assistance to those in need, in subordination to the ruling authority and in compliance with the applicable rules of law"* (Police Law, 2012). The task is specified in three sub tasks: maintaining public order (under the command of the major), criminal law enforcement (under command of the prosecutor) and helping those in need of assistance. To carry out these tasks, police officers have the possibility to use force or freedom restricting means, also known as the police monopoly on the legitimate use of force. This is an essential theme that forms the starting point for this research. What does the police authority to use legitimate force entail and does it encompass cyberspace? Let us first have a look at recent news coverage of a real-life policing example:

Figure 1: [Riot police in action Amsterdam 2015]. Copyright holder unknown. Retrieved from http://media.nu.nl/m/m1oxq59at6gh_wd640.jpg/me-ontruimt-maagdenhuis-in-amsterdam.jpg

Amsterdam, April 11th, 2015: Around ten o'clock the riot police arrive at the university building that students have occupied since the 25th of February. They use a megaphone to instruct the students to leave the building immediately. After ignoring this instruction, riot police units clear the building, using physical force where needed. At the same moment, horseback police wipe the adjacent square. Nine protesters are arrested, for insulting and obstructing police officers, and throwing a paint bomb to a police horse. Some arrested students are released a little while later (Volkskrant, 2015).

Not many people would be very surprised after reading the above news item: Dutch police have (together with a number of other, smaller parties) the authority to use legitimate force within the country borders and the above case is one of the many examples of how it is applied. Although the police are regularly criticized about how it is used (NRC next, 2013; AD, 2014; Trouw, 2015), the sheer fact that they have this authority is undisputed.

Figure 2: [The Eel insurgence](n.d.). Copyright holder unknown. Retrieved from http://www.jordaanmuseum.nl/palingoproer.jpg

This central role in the application of force hasn't always been this significant. Although the tasks of justice and law maintenance go back ages, a recognizable and organized police organization has been around for about two centuries, established during the French annexation of the Netherlands (1810-1813). At that time a municipal police was established in the cities, and the ranks of commissioner, inspector and constable were introduced, as well as a separate field watch in the rural area and a generic police after the example of the French Gendarmerie (Breukers, n.d., pp. 11-12). However, up to the beginning of the

20th century, the Dutch military still had a very important role when force was needed for public order management. Some famous examples are the Eel insurgence ("Palingoproer") and the Potato insurgence ("Aardappeloproer").

The first took place in 1886, in a working class neighborhood in Amsterdam, called the Jordaan, against the background of a growing social-democratic movement and discontent about working and living conditions. The riot started when the forbidden game of "eel pulling" was played, and the police wanted to end it. This incident ignited the spark and led to an outright uprising. Police forces were bombarded with stones, flowerpots and pieces of iron. The number of wounded policemen increased by the hour, and they couldn't gain control of the situation. A specialized riot police didn't exist yet at the time, so the army was called. Cavalry, infantry, hussars and marines arrived in the small streets and showed their muscles. The riots resulted in 26 deaths, 36 severely injured, and 100 slightly injured (Van der Wal, 2003, Pp.164- 172).

The second incident, the Potato insurgence, took place in 1917, once again in Amsterdam. Because of a famine the people started to ransack food and potato warehouses. The police couldn't handle the estimated 15-20.000 rioters and asked for military assistance. Special trains brought hussars, infantrymen and troopers to Amsterdam, who entered the streets with considerable display of power. The incident led to ten deaths and 113 people were wounded (Van der Wal, 2003, pp. 274-277).

The blunt and in many cases deadly methods of the military contributed to a gradual change in the use of force during public order management, increasing the role of the police and minimizing the role of the military (van der Wal, 2003). This process took a long time to come to fruition. Important moments in the 20th century are 1966 and 1969. In 1966, a strike in Amsterdam amongst construction workers got out of hand, with many rebelling youngsters joining the riots. The ill prepared riot police in Amsterdam was not ready for this and could not curtail the situation. In 1969 there was another uncomfortable situation for the riot police: students occupied the university building "Maagdenhuis" in Amsterdam and the police had trouble finding a suitable way to deal with this. These and other demonstrations in university towns led to new plans for the Dutch police to professionalize riot police and public order policing: at the time, the riot police were often led by commanders who had received no training, resulting in constantly changing tactics and demotivation among police officers. Despite the good intentions, riots in the 1970's and the coronation riots of 1980 showed out that the professionalization was not implemented as planned (Fijnaut, 2008). Finally, during the last three decades the riot police did develop into a more professional apparatus with a better track record when it comes to proportional use of force than in earlier times (Adang, 2009, pp. 89-90)

Another illustration of the long and winding road on the history of force use is the police belt. You would say that this is a very simple object, but the enormous amount of changes that it went through proves otherwise. According to Meershoek (2012, p. 2), the depots of the police museum in the Netherlands show hundreds of different models. This shows that the types and number of weapons available to the police, in plain sight or covered, have been subject to change for a very long time, and still are. All these different belts are snapshots of different moments in time in which the political and societal developments, as well as preferences of officers, are reflected in the changing object. This reminds us that the number and type of weapons police have to their disposal is not something static: they come, they go and they change.

1.2 Current use and instruction on the use of force (*"geweldsinstructie"*) and the absence of offensive cyber capabilities

The authorization to use force is captured in the Dutch Police Law. Article 7, chapter 1 says: *The police officer who is appointed for fulfillment of the policing task, is authorized to use legitimate force or freedom restricting means, when, considering the associated risks, this is justified by the intended purpose, and this purpose cannot be accomplished in any other way. If possible, the police officer issues a warning prior to the use of force (*Police law, 2012*).*

An important addition: the authorization only applies inside the jurisdiction of the Netherlands, not in the territories of other sovereign states, as explained in the territoriality principle. This is described in article 8 of the Law of General Provisions (Wet Algemene Bepalingen, n.d.) that can be translated as "The penal codes and regulations of the police are binding to all that are within the territory of the Kingdom" [1] and as well in the Dutch Penal code, article 2: "The Dutch criminal law applies to any person who is guilty of any criminal offense in the Netherlands" [2] *(*Wetboek van Strafrecht, n.d.).

To be able to legitimately exercise this authority, the Dutch police have a detailed instruction for use of force (*geweldsinstructie"*), which is included in the official instruction for the police, royal constabulary and extra-ordinary investigative officers. The instruction describes by whom, when and how force may be exercised. Force is defined as: *"any coercive power of more than slight significance applied to persons or goods"* (Dutch government, 1994)

The force can be applied defensively (e.g. to stop an aggressive suspect) as well as offensively (e.g. to assault and shoot a terrorist) . Very important principles when it comes to the use of force are proportionality and subsidiarity. Proportionality means that the amount or type of force that is applied should be proportional in risk and effects considering the intended purpose. Subsidiarity means that there are no better suited alternative options to reach the intended purpose (Naeyé, 2005).

Apart from their own physique (punching, strangulation, kicking etc.), the police have a number of instruments at their disposal to apply force successfully; most important are the pepper spray, the short baton, the long baton, the pistol and the surveillance dog. Besides these, improvised objects can be used when a situation requires it. Police researcher Naeyé (2005) conducted a study about all police use of force in the year 2000. In this study, 135 incidents showed improvised objects used to apply force. A quarter of these involved the flashlight (Maglite) or police radio. Other examples are the police car (for a controlled collision) and an iron pipe.

Interestingly, both official instructions and the sizable body of literature about police use of force lack the use of force in cyberspace. Force is always seen in the physical form (Naeyé, 2005; Drenth, Naeyé & Bleijendaal, 2008; Bleijendaal, Naeyé, Chattellon & Drenth, 2008; Dutch Government, 1994).

1.3 Pre-conclusion

The Dutch police are granted authority to use legitimate force. Police officers have a number of instruments at their disposal to apply force, and police organizations have specialized riot police units.

---

[1] *"De strafwetten en de verordeningen van policie, zijn verbindende voor allen die zich op het grondgebied van het Koningrijk bevinden"*

[2] *"De Nederlandse strafwet is toepasselijk op ieder die zich in Nederland aan enig strafbaar feit schuldig maakt"*

A detailed instruction about the use of force describes by whom, when and how force should be exercised. Two terms that should be kept in mind for later chapters of this thesis are proportionality and subsidiarity. These should also be leading principles when considering use of force in cyberspace. Furthermore, it seems that the police use of force hasn't been associated with cyberspace yet; the instruction doesn't say anything about it. Section 1.1 shows that it took a long time for the Dutch police to obtain their central role in the application of physical force. Before that, the Dutch military gave assistance when needed, resulting in disproportionate and in many occasions deadly actions. Will the road to successful enforcement in cyberspace be long as well?

In the next chapter we will look at cyberspace and why offensive cyber capabilities would be interesting to explore.

2. Cyberspace and the difficulties of criminal investigation

Chapter one showed that Dutch police are granted authority to use legitimate force, and has detailed instructions for using it, but not in cyberspace. As was stated in the introduction, this thesis propagates that the Dutch police start exploring the use of force in cyberspace. Chapter two covers the question why this should happen: what is 'cyberspace', what role does it play in contemporary society, should the police carry out their task in cyberspace, and what difficulties arise when the police conduct investigations in cyberspace? Finally, in section 2.3 of this chapter, the strategy of disruption and its suitability to tackle cybercrime is examined.

2.1 The omnipresence and importance of cyberspace

The term 'cyberspace' was introduced in 1982 by science fiction author William Gibson in his short story 'Burning Chrome', and later appeared in other books as well. In these so called "cyberpunk" novels, the word is used to describe a digital, three dimensional space that can be roamed, and it gives an adventurous, wild-west like feeling. As with many science fiction predictions, authors in the cyberpunk theme were a bit too optimistic, which is illustrated by the following quote: *"In the 20th century, the Net was only accessible via a computer terminal, using a device called a modem to send and receive information. But in 2013, the Net can be entered directly using your own brain, neural plugs and complex interface programs that turn computer data into perceptual events. (Pondsmith, 1988 in Birch & Buck, 1991, p. 1)"*

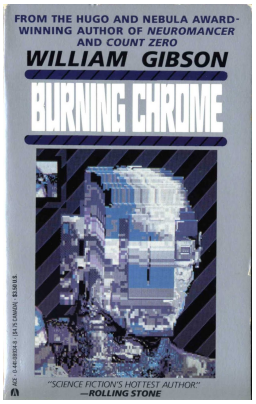


Figure 3: 1987 Paperback cover of Burning Chrome. Retrieved from http://theporporbooksblog.blogspot.nl

This thesis though, is not about the fictional cyberspace from the previous century, but about the real world cyberspace in the year 2016. So let's have a look at the Oxford English Dictionary. This defines cyberspace as: "*The notional environment in which communication over computer networks occurs*" (Coe, 2015), which is quite broad and open for a multitude of interpretations. Definitions from the field of cyber security are more precise: according to the British Cyber Security Strategy, cyberspace is '*an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the Internet, but also the other information systems that support our business, infrastructure and services.*' (United Kingdom government, 2011) The Dutch Cyber Security Strategy, version 2013, mentions cyberspace only once and generally uses the term 'cyber domain', which is described as: *'the conglomerate of ICT goods- and services which encompasses all entities that (can be) digitally connected. The domain includes permanent as well as temporary or local connections, and data, program code and information that is located in the domain, with no geographical limitations."* (The Netherlands government, 2013, p. 7)

Figure 4: Cyberspace in the movie "Johnny Mnemonic", based on a book from William Gibson. Retrieved from http://os.typepad.com/my_weblog/Internet/

This definition is atypical, when compared with all others: the authors also include non-connected devices, such as USB devices and offline computer systems. We can also find definitions in the academic world: Yar (2006, p.155) defines cyberspace as: "The interactional space or environment created by linking computers together into a communication network." Rowland, Rice and Shenoi (2014) use the following definition: "the ever-expanding manifestation of the pervasive information and communications infrastructure". In this thesis the

definition of cyber domain from the Dutch Cyber Security Strategy will be used because it is precise and focused on the Netherlands.

A concept that is strongly interwoven with cyberspace is the Internet. Although cyberspace is generally seen as more comprehensive than the Internet, a cyberspace without the Internet would be hard to imagine.

Its origins were developed in the early 1960's, during the heydays of the cold war between the United States and the Soviet Union. A number of authors explored concepts that would later form starting principles for the Internet. Kleinrock (1961) wrote a first paper on packet-switching technology. Licklider & Clark (1962) came up with the idea of using a globally interconnected set of computers as communication device, describing a concept much like our modern Internet.

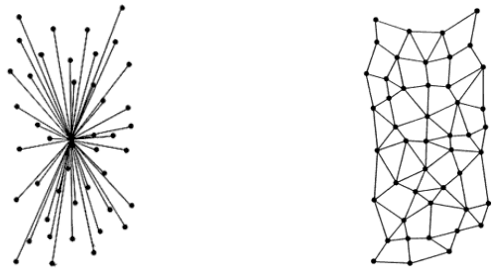


Figure 5: Centralized and decentralized networks. Retrieved from http://www.rand.org/about/history/baran.html

Paul Baran (1964) from RAND Corporation came up with an idea to communicate in the aftermath of a nuclear war. The communication systems in use up to that moment were based on a centralized switching facility, which would not survive a nuclear attack. Baran's idea was to create a system with distributed instead of centralized switches, so it could still operate in case a number of switching nodes were destroyed by an attack (Baran, 1964). The ideas of Kleinrock, Licklider and Baran formed the basis for development of the ARPANET, a system that was adopted and funded by the Defense Advanced Research Project Agency (DARPA). Its first permanent link was established in 1969 and within two years it (unexpectedly) turned into a high-speed electronic post office for exchanging everything, from technical to personal information. In 1989, ARPANET changed into the "Internet" (Leiner et al., 2009; Rand Corporation website, n.d.). In the same year, the World Wide Web (WWW) was invented, a universal multimedia communications network. Web browsers and search engines were developed, and the rest is history. The Internet has shown the fastest rate of penetration of any communication medium that ever existed, many times faster than radio and TV (Castells, 2009, pp. 50-51).
Nowadays, the Internet and World Wide Web are the foundation of the broader term cyberspace. What does cyberspace mean for society, the way we live our lives? This is an interesting theme, on which sociologists expressed their views. Many of them give cyberspace a central role in contemporary society. Castells (2009) sees a radical change in the realm of communication: a shift from traditional mass media to a system of horizontal communication networks organized around the Internet and wireless communication. This results in a fundamental cultural transformation, because virtuality becomes *"an essential dimension of our reality"* (Castells, 2009, p. 18). He also describes the characteristics of relations in the Internet, which are particularly suited for the development of so-called "weak ties", that are useful in providing information and opening up opportunities at a

low cost. These enable interacting with strangers, while social characteristics are less influential in framing or blocking communication. So cyberspace changes interpersonal relationships: it allows communities to overcome distance at low cost, combines the speed of mass media with the pervasiveness of personal communication, and allows multiple memberships in partial communities (Castells, 2009, pp. 388-389). In the book "moral blindness" from Zygmunt Bauman and Leonidas Donskis (2013), the authors mention generation Y (1985-1995) as the first generation to enter a world already containing the Internet and to know and practice digital communication in real time. They are unequalled masters of surfing online and at being "connected" while their number of friends (on social media) is in the hundreds, if not thousands. (Bauman & Donskis, 2013, pp. 152-153). Their analysis shows the central and important role of cyberspace in our social life and especially that of the younger generations. Cyberspace is omnipresent and we are always online.

Apart from the change in culture and communication, cyberspace also changes the way we do business. A survey from Bradley, Loucks, Macaulay, Noronha & Wade (2015), shows how "digital disruption" reshapes markets. The respondents of their survey, executives of large and midsized private sector companies, believe that four out of the top ten companies per industry will be displaced in the next five years. The best way to describe this, according to the authors, is as a "digital vortex", that draws everything to it's area of influence, *"in which business models, offerings, and value chains are digitized to the maximum extent possible"* (Bradley et al., 2015, p. 5). The disruptors innovate quickly, gaining market share and scaling far faster than competitors still holding on to physical business models. A striking example is that of communication application WhatsApp, which grows at a staggering speed, displacing the Short-Message-Service (SMS) entirely.

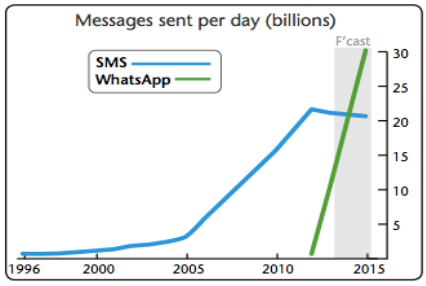


Figure 6: Number of messages sent per day with SMS and Whatsapp. Reprinted from "Digital Vortex: How Digital Disruption is Redefining Industries," by J. Bradley, J. Loucks, J. Macaulay, A. Noronha & M. Wade, 2015. Retrieved from http://www.imd.org/uupload/IMD.WebSite/DBT/Digital_Vortex_06182015.pdf

According to Castells (2009, p. 391), the popularity of on-line shopping is exploding; some traditional stores (for example, bookstores, record stores, perhaps car dealers) will be either phased out or transformed by on-line competition. Recent figures from the Netherlands confirm this: in 2014, Dutch consumers spent 13.9 billion Euros online. 7 billion was spent on products, which represents 10% of the total product sales in the country. The other 6.9 billion was spent on services, a whopping two third of all expenses on services. Examples of digital disruption in the Netherlands are the bankruptcy of the retail concerns Schoenenreus (2015, shoes, 206 stores), Mexx (2014, fashion, 315 stores) and Free Record Shop (2014, entertainment, 177 stores). The failure to embrace a successful on-line strategy is seen as an important cause for this (Koetsenruyter, 2014; website www.nu.nl).

We seem to reach a threshold where the number and importance of our actions and our communication in cyberspace equal or even surpass those in the physical world. Crime also shifts from the physical world to cyberspace. The number of victims of cybercrime in the Netherlands is substantial and growing (Centraal Plan Bureau, 2016; Domenie, Leukfeldt, van Wilsem, Jansen & Stol, 2013). These are important findings for this thesis, it shows that the police task must also be carried out in cyberspace. One way to do this is criminal investigation under the command of a prosecutor, which has already been done for a while. In the next section we look at criminal investigation in cyberspace and the difficulties that arise.

2.2 Two criminal phenomena in cyberspace and the difficulties of investigation

To point out the difficulties that the police encounter when investigating and prosecuting criminals in cyberspace, two criminal phenomena are examined: (Distributed) Denial of Service ((D)DoS) attacks and illegal trade on The Onion Router (TOR) hidden services. The first can be characterized as a cybercrime, the second as a cyber-enabled crime (also known as computer-facilitated crime)(NCSC, 2012).

Cybercrime, also known as narrow cybercrime, is defined on the website of the Dutch police (https://www.politie.nl) as: "*crime with Information and Communication Technology as means and target*". The Dutch National Cyber Security Centre (2012, p.11) defines it as *"criminal behavior that cannot be performed without the use of information communications technology (ICT). Typical for narrow cybercrime is that hardware, software or equipment and the data that is stored on that are the goal of the perpetrator."*

Cyber-enabled crime, also known as broad cyber crime, is defined by Mc Guire and Dowling (2013) as follows: *"traditional crimes, which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT). Unlike cyber-dependent crimes, they can be committed without the use of ICT."*

The most important distinction between cybercrime and cyber-enabled crime seems whether or not both the attack and target are in the domain of information and communications technology. While cyber-enabled crimes are mostly traditional crimes that make use of information and communications technology, cybercrimes do not have analogues in traditional crimes (Strikwerda, 2014, p.19).

This chapter starts with examining (D)Dos attacks, its characteristics and the difficulties that arise in criminal investigations. The first paragraph (2.2.1) contains literature study about (D)DoS attacks and about illegal trade on TOR hidden services, and the second paragraph (2.2.2) shows the results of a survey amongst high tech crime investigators, about the difficulties of cyber investigations, are presented.

2.2.1 (D)DoS attacks and Illegal trade on TOR hidden services

D(D)oS Attacks

The (Distributed) Denial of Service attack is described by Coleman (2014, p. 3) as a tactic to disrupt access to webpages by flooding them with tidal waves of requests. Sauter (2014) describes it as an action that seeks to render a server unusable to anyone looking to communicate with it for legitimate purposes. A Denial of Service Attack (DoS) comes from one source, a *Distributed* Denial of Service Attack (DDoS) comes from a number of computers, preferably on different networks. The latter can be computers of a group of volunteering individuals, but also "zombie" computers in a botnet. These are (often without knowledge of the owner) infected and kidnapped by malicious software and mostly directed by a command and control server. Botnets can contain up to millions of zombie computers (Europol, 2015), and many of them can be rented at relatively low cost through black markets (Segura & Lahuerta, 2010, p. 8).

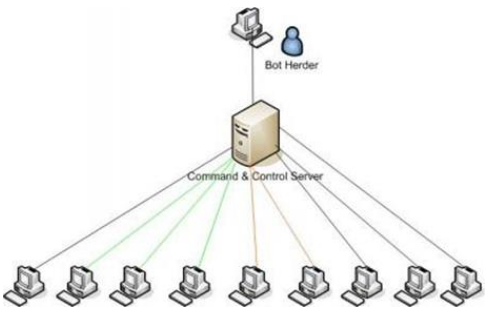


Figure 7: Graphical representation of a botnet with Command & Control Server. Retrieved from http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/040813_1107_Botnetsandc2.jpg

One of the most popular attacks is the DNS amplification attack. This sends (spoofed) request to DNS resolvers to flood a target with responses. Its popularity is probably due to the fact that a relatively small DNS request of

a few bytes can result in a much larger DNS response, which is sent to the target (Herzberg, 2014, p. 1). Amplification based on the User Datagram Protocol (UDP) is also gaining popularity. Spoofing UDP traffic is relatively simple and the attacks can be very powerful (NCSC, 2014).

Conducting a (D)DoS attack is punishable by article 161sexies in the Dutch penal code: *"he who willingly destroys, damages or disables any automated work or work for telecommunication, or causes a hindrance in the functioning of such work, or foils a security measure of such work."* (D)DoS attacks can be used for various goals and by various types of perpetrator: to extort people (*"pay us now or get (D)DoS'd"*), to molest a competitors website, to denounce an ideological issue (also called hacktivism) or just for the lulz[3] of it. Hacktivism can be described as "civil disobedience", willfully breaking the law to your cause, while risking imprisonment (Sauter, 2014, p. 21). Famous examples of civil disobedience are the lunchroom sit-ins, peaceful street marches and Rosa Parks sitting in front of the bus by the Afro American Civil Rights Movement in the 1950s and 1960s.

The most famous example of hacktivists performing (D)DoS is Anonymous. The two main "cyberweapons" used to perform the (D)DoS attacks were botnets (as described above) and the Low Orbit Ion Cannon (LOIC). The LOIC is a tool that allows users to send useless requests or "packets" to a server of choice automatically. If many people used the tool simultaneously, they could overload a web site with enough traffic to take it offline (Olson, 2012, p. 75-77).

Opposed to hacktivist (D)DoS attacks, extortion (D)DoS attacks are much less idealistic. These kind of attacks are meant to collect extortion money. Attackers threaten to DDoS companies if they do not pay a ransom. Typically, the ransom must be payed in Bitcoins. According to Perlroth (2014), tech startups are a popular target for these kinds of attacks, because of their dependence on around-the-clock Internet access for their livelihood.

Illegal trade on The Onion Router

The second phenomenon is illegal trade on TOR hidden services. TOR stands for "The Onion Router". It was invented under the flag of the US Naval Research Laboratory. (Goldschlag, Reed & Syverson, 1999). Onion Routing was introduced in 1999 as an "infrastructure for private communication over a public network" (Goldschlag et al., 1999, p. 1). It builds anonymous connections based on so called "Chaum Mixes", invented quite some time earlier, in 1981 (Chaum, 1981). The Mixes receive messages from numerous sources, perform cryptographic transformations on them and then forward them in random order to the next destination. When using a numerous amount of these, determining who is talking to whom becomes very difficult. The TOR system combines this with creating "onions". These are layered data structures that specify properties of the connection at each point along the route. As the data package moves through the anonymous connections, each router removes one layer of encryption, similar to peeling off layers of an onion; hence the name. Finally, the receiver gets the message unencrypted. The return message moving backward will also start as an onion, only with a different algorithm and key.

Although the TOR infrastructure was introduced in 1999, it took a long time before it became known to the masses. In 2004, programmers rewrote the code to make it easier to use and developed a client program so that users could send data from their desktop computers (Dingledine & Mathewson, 2004). This led to publication of an article about the browser in Wired magazine, raising awareness of TOR (Zetter, 2005). But the real leap in TOR usage took place around 2010.

[3] Lulz is a corruption of LOL, which stands for "Laugh Out Loud," signifying laughter at someone else's expense (Coleman, 2014, p. 30).

The anonymity that TOR provides combined with the user-friendly browser resulted in a large user base, serving for different purposes. A good way to describe the user base of TOR is "The Good, the Bad and the Ugly". The "Good" stands for all TOR users in repressive regimes that are not too concerned with human rights. In some countries, for example China and Iran, Internet pages are actively monitored and/or censored (Taneja & Wu, 2014; Yang & Liu, 2014; Rahimi, 2015). TOR can evade this, so dissidents are still able to express their opinions and visit sites that interest them. The "Bad" stands for the people that use TOR to conduct criminal activities. Because of TOR's anonymization capabilities, a thriving market offering all imaginable illegal goods and services emerged. Lastly, the "Ugly" stands for people in the community around producing and consuming child pornography who also reap the benefits of TOR. These are criminal activities as well, but with a different type of perpetrators than dark markets. This conduct is loathed by the general public, hence the name "ugly". Websites for illegal trade on the TOR hidden services are also known as "dark markets". The conduct is cyber-enabled crime, punishable by a number of articles in Dutch laws, depending on the goods and services that are sold. Most illegal trade consists of drugs, covered by Dutch Opium Law. Other possibilities are counterfeiting (article 210 Dutch Penal Code), forged passports and other forged documents (article 225 Dutch Penal Code) or sale of intellectual property (article 31-32 Dutch Copyright Law). The first and best known dark market was "the Silk Road". This marketplace, shut down by law enforcement in 2011, offered a large collection of softdrugs, hard drugs, counterfeit goods and money, illegal software and forbidden books. After the website had been shut down and its owners arrested, new dark markets popped up on the TOR web like mushrooms. At the moment, the number of openly promoted markets is close to forty (www.deepdotweb.com). This is not all: some dark markets are local and invitation only.

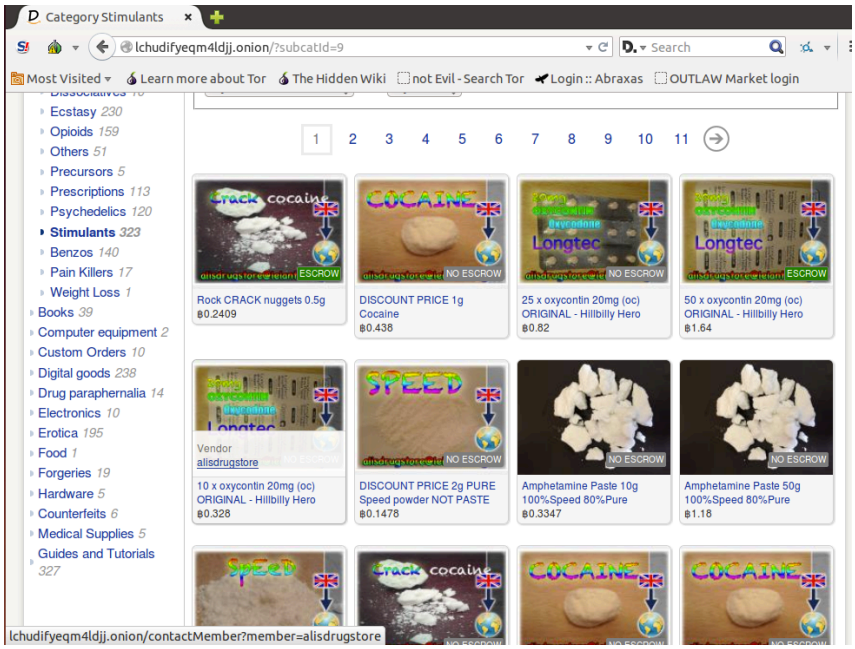


Figure 8: Drug offerings on a dark market. Retrieved from lchudifyeqm4ldjj.onion

2.2.2 Survey: difficulties of investigating (D)DoS and illegal trade on TOR hidden services

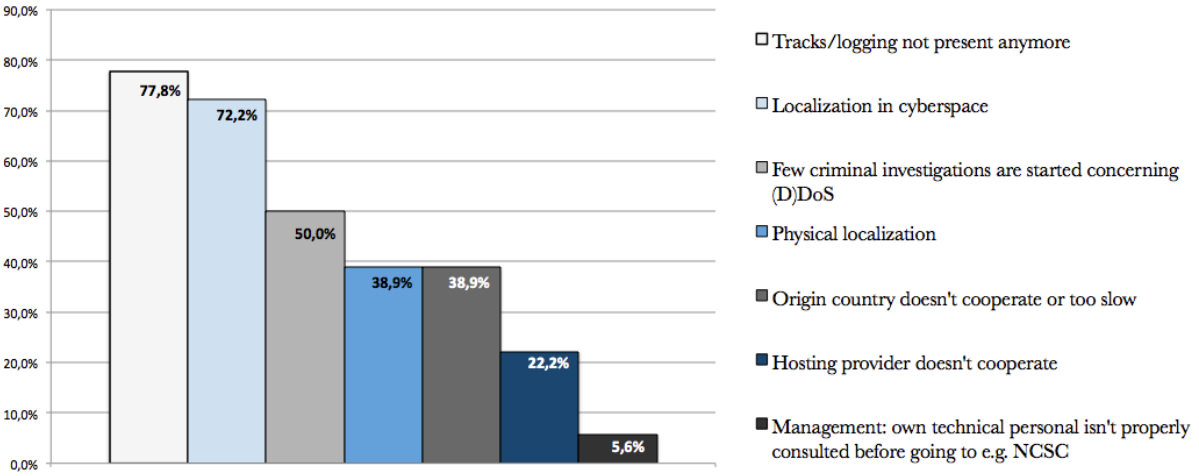
Both (D)DoS attacks and illegal trade on TOR hidden services are crimes. One strategy to fight crimes is to conduct criminal investigations, detecting and prosecuting the criminals behind it. However, a number of technical possibilities stand in the way of successful investigations.

To get a better look at the difficulties that arise during these investigations, a survey was conducted among employees of the Dutch National High Tech Crime Unit. This survey was sent to all 117 officers in the

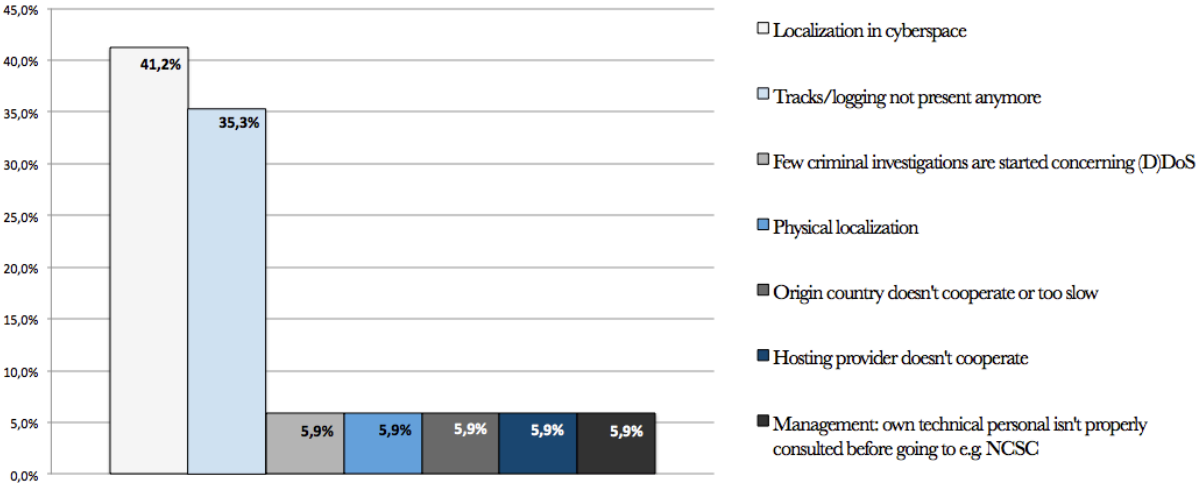
department (tactical investigators, digital investigators, dossier makers and advisors). The survey has an N of 24 and the response rate was 20,5.

The survey plainly shows that the two most serious obstacles when investigating (D)DoS attacks are the absence of tracks and logging, and the difficulties to localize the origin of the attack in cyberspace. The biggest obstacles when investigating illegal trade on TOR hidden services are the physical localization of the hidden service (locating the server) and the identification of buyers and sellers on TOR hidden services (coupling the cyber identity to a real world identity).

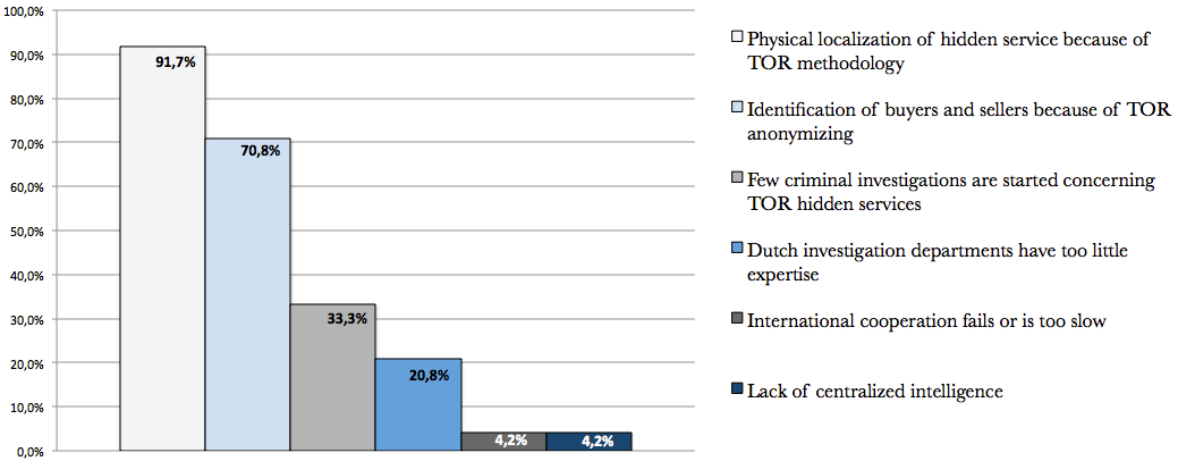
Question 1: What obstacles do the Dutch police encounter during the criminal investigation of (D)DoS attacks?



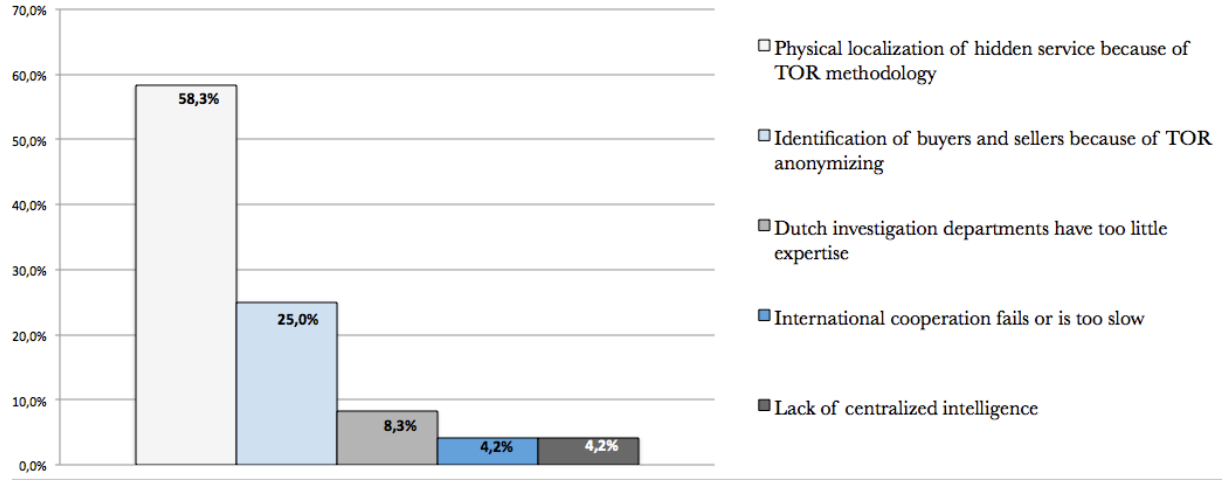
Question 2: What is the biggest obstacle that the Dutch police encounter during the criminal investigation of (D)DoS attacks?



Question 3: What obstacles do the Dutch police encounter during the criminal investigation of illegal trade on TOR hidden services?



Question 4: What is the biggest obstacle that the Dutch police encounter during the criminal investigation of illegal trade on TOR hidden services?



2.3 The disruption alternative

The previous section showed difficulties criminal investigators in cyberspace run into. New anonymization technologies make it hard to link cybercrimes to real identities in the physical world that can be prosecuted. The technologies that were mentioned are only part of the arsenal: spoofing addresses, Virtual Private Networks (VPN), encryption and bulletproof hosting providers are other available techniques (Brunner, 2015). Because of these difficulties, it could be interesting to look for alternatives to combat crime in cyberspace.

One of these alternatives is a disruption strategy: looking for ways to disturb criminal processes. The strategy of disruption is already widely used by the Dutch Police, the thoughts behind it were introduced around 2003, in a report called "Obstruction as Asset" (originally "Tegenhouden Troef", in Dutch)(Projectgroep Opsporing-2, 2003). The report was written under the authority of the Dutch Counsel of police chiefs. They define the concept

of disruption ("tegenhouden" in Dutch) as follows: *"The influence of such behavior and circumstances that prevent crime and other breaches of security and social integrity"* [4].

This seems to offer opportunities for the police in cyberspace. Since investigation is getting more difficult, they could try to influence circumstances to prevent and disrupt crime in cyberspace. However, when we look for disruption in the law, it is hard to find anything.

A Dutch law student who wrote a master thesis about the disruption strategy in 2007, agreed on that. Although the thesis focuses on disruption in the physical world, he already concluded that there was a lack of legal basis for the disruption strategy. He stated that especially the definition and limitations of the term disruption should be included in the law, and that the distinction between disruptive activities on behalf of the public order, on behalf of criminal law enforcement and on behalf of terrorism prevention should be specified (Verpaalen, 2007, p. 41).

Even though disruption is a broad definition, and leaves many question marks about its legality, it does offer an interesting alternative to criminal investigation and prosecution in cyberspace. Therefore, specific attention will be paid to the possibility of using enforcement methods in cyberspace for disruptive activities.

2.4 Pre-conclusion

This chapter discussed the impressive speed with which "cyber" became an undeniable aspect of our lives.

We are always online and the importance of our actions and our communication in cyberspace equal those in the physical world.

We looked at (D)DoS attacks and illegal trade on TOR hidden services and conducted a survey that shows how difficult criminal investigation of these crimes is, due to techniques that hide the location and identity of the criminal. These are only two examples of crimes that heavily rely on information and communication technology and largely take place in cyberspace. Other crimes, such as child porn, terrorism and e-fraud pose the same kind of difficulties, and undoubtedly new types of (cyber) crime will follow in the future. Due to the difficulties of investigation and prosecution, it can be interesting to look at the alternative strategy of disruption: trying to influence circumstances to prevent and disrupt crime. We will look at enforcement methods in cyberspace with that strategy in mind. But beforehand, it is important to answer the following question: can the authority to use legitimate force be translated to cyberspace?

[4] In Dutch: *"het zodanig beinvloeden van gedrag en van omstandigheden, dat criminaliteit of andere inbreuken op de veiligheid en de maatschappelijke integriteit worden voorkomen"*

3. The authority to use legitimate force in cyberspace

3.1 Translating the police authority to use force to cyberspace

Chapter one showed that the Dutch police have quite a history with force in the physical world. After good and bad experiences, there is now a situation in which the authority to use (physical) force is generally accepted, embedded in laws and described further in official instructions. All this is not the case for the use of force in cyberspace: the history of police force in cyberspace is still to begin. This section makes a first step by answering sub-question 5: is the police authority to use legitimate force also applicable to cyberspace?

Since we need to find out whether the police authority to use force also applies to cyberspace, we need to look at the current definition of the use of force and the official instructions once more:
The Dutch Police Law: "*the police officer who is appointed for fulfillment of the policing task, is authorized to use legitimate force or freedom restricting means, when, considering the associated risks, this is justified by the intended purpose, and this purpose cannot be accomplished in any other way. If possible, the police officer issues a warning prior to the use of force.*" (Police law, 2012)
The Official instructions for police, royal constabulary and other investigation officers: *"force: any coercive power of more than slight significance applied to persons or goods"* (Dutch government, 1994)
So, police officers are authorized to use legitimate force or freedom restricting means to persons or goods.

This research will focus on force or freedom restricting means in cyberspace, with targets in the cyber domain defined in chapter 2 as: *'the conglomerate of ICT goods- and services which encompasses all entities that (can be) digitally connected; permanent as well as temporary or local connections, and data, program code and information that is located in the domain".*
The question is: can these "goods", the bits and parts that make up cyberspace be interpreted as "goods" as seen in the official instruction for the use of force? If so, the current definition of the police authority to use force also applies to cyberspace. If not, the law will need to be changed to use enforcement in cyberspace.

This results in the following null hypothesis:
H_0: permanent as well as temporary or local connections, and data, program code and information can be seen as goods.

Since offensive actions in cyberspace are not mentioned anywhere in the Police Law or in the official instructions we need to look elsewhere for guiding principles, for example the Dutch Supreme Court. In a case from 1921, the Electricity arrest, the judges of that court concluded that electricity should be seen as a good, stating that also non-material objects can be seen as goods. Their final verdict included the following text:
"this electricity, although its presence may only be established in connection with something tangible, can be transmitted through human activity on another matter and can even be accumulated; furthermore, it can be generated by human activity and remains available to those who produced it. It represents a certain value for them, on the one hand because its production was associated with expense and effort, secondly because they can use it for their own benefit and thirdly because it can be transferred to others for a fee" (Supreme Court, 23 May, 1921, NJ 1921/564, p. 568).

In this case, the word electricity can easily be replaced with connections, data, program code and information, so far the null hypothesis cannot be rejected.
We will now make a leap to the end of the previous century. Computers and data were on the rise, the information age was starting and that already fueled discussions about our research question: can data be seen as goods? In 1989, Groenhuijsen and Wiemans wrote an article with a thorough analysis of this discussion. In the article they also summarized a meeting of the Dutch Jurist Association in 1988 in which this question was discussed. During the end vote, the meeting concluded that data cannot be seen as goods (Groenhuisjen & Wiemans, pp. 96-100).
Supporters of that perspective argue that there is at least a problem with the transferability of data; they are not "unique" but "multiple". Many people can simultaneously have access to the same data. It could therefore become problematic when one wants to seize them and deprive the owner of property, since there can be copies on different places. They add that data are the product of mental labor, while goods are the product of physical labor (Kaspersen in Koops, 2007, pp. 19-20). In 1996, the Supreme Court judged in accordance with that. In a case in Aruba, they found the suspect guilty of appropriating digital data on floppy disks belonging to his former employer. But they base their decision on the fact that the data carrier, the floppy disk, is the good, and not the data itself. In their judgment they use the argument that was described above: *"a "good", as meant in legal definitions should have the essential characteristic that whoever has the actual power over it, necessarily loses this when someone else obtains this power. Computer data lack this characteristic"* (Supreme Court, 3 December 1996, NJ 1997/574, p. 3093).

In later cases the disposition of judges shifted again. In a case known as the Runescape judgment two under age boys physically attacked and restrained another underage boy while misusing his game account to transfer virtual items to their own game characters. Eventually, the Dutch Supreme Court convicted them for theft (Supreme court, 31 January 2012, ECLI: NL: HR: 2012: BQ9251). In a similar case, the Habbo judgment, that concerned stealing of virtual goods from the game "Habbo Hotel", the verdict of the Court of Amsterdam was also theft (Court of Amsterdam, 2 April 2009, ECLI:NL:RBAMS:2009:BH9791).

In the Runescape judgment, The Supreme Court also analyzed whether the virtual items in the game can be seen as "goods", which is useful for our hypothesis. They state that since 1921 (the Electricity arrest), the need for a good to be physical was dropped. On top of that, they point out that the economic concept of value became more subjective and relative in case law throughout the years. Most relevant is the value the good has for the owner. In the end, the court states that *"all things considered, the court deems that as a consequence of the digitization of society, a virtual reality arose, that cannot be dismissed as mere illusion, for which the committing of crimes would not be possible".*
So also virtual items in computer games, which only consist of bytes stored on a computer somewhere, can be seen as "goods".
Koops (2014) has some doubts about this argumentation, stating that it opens the door to a very casuistic way of reasoning about whether certain data behaves as "data" or as "good".

However, since there is no other legal basis to hold on to as yet and considering the scope of this thesis, the above judgment from the Supreme Court is sufficient to confirm the null hypothesis. That also means that we hold on to the assumption that the police authority to use legitimate force is applicable to cyberspace. Logically, the question still needs to be fully addressed by legal experts since all former legal discussions about data as "goods"

were from the perspective of theft and appropriation, not from the perspective of police force against these "goods" in cyberspace.
The respondents in this thesis were also asked the question whether the police authority to use force applies to cyberspace. They unanimously agreed with this. But how this should be executed, resulted in a variety of conceptions. A legal expert explains:

"With this type of action you exercise such a degree of force that things cannot function the way they should. You can define that as force, so you can consider this being part of the police monopoly of force. If we all agree about that, we can say: "This is force, from now on." Or perhaps we should expand the definition with virtual affairs. I believe this is the least problem of all."

A respondent points out that the police should claim the digital public order and criminal law enforcement. If they fail, others will take over, for example private parties. He states that if someone uses enforcement methods in cyberspace, it should be the police, and not a private company or another agency such as the National Cyber Security Centre.

"I would not give such tasks to the NCSC. We should not have another institute with executive powers. If these methods are used against criminal conduct it should be a police authority. The NCSC is mainly meant to perform defensive work in their relationship with vital parties. This disruption idea is more on the perpetrator side, and in my opinion that is clearly police work." Cyber Security Expert

A cyber security expert finds it obvious that the authority to use force is also applicable to cyberspace, since the digital world is becoming ever more important. Contemporary life takes place as much in the digital as in the physical world, and these two worlds are becoming more and more intertwined. You make all kinds of transactions in the digital world, which also affect the physical world; you can no longer see the difference. It is a direct extension of the real world.
The translation of the authority to use force to cyberspace fits in with the motto that was first used nearly twenty years ago in the Netherlands: "What applies offline must also apply online." It was mentioned in a report from 1998, called "The Electronic Highway". It was written by a number of academics, on behalf of the government. In this report, the writers handle the basic principle that the judicial norms from the physical world should also be applicable in the electronic domain (Dutch government, 1998). So basically this is what the government has already proclaimed for a long time.

3.2 Pre-conclusion

The analysis in this chapter looked into the definition of the use of force and the corresponding official instructions and demonstrated that the police authority to use legitimate force is also applicable to cyberspace. Rulings from the Dutch Supreme Court show that connections, data, program code and information can be seen as "goods", on which the police can apply force.
So, in line with a conclusion from a government report from 1998, what applies offline must also apply online. In this case that involves the police authority to use force.
But if the police are to start enforcing the law in cyberspace, this cannot happen overnight. There will be a number of legal and ethical considerations and challenges. These will be discussed in the following chapter.

4. Possibilities and constraints of law enforcement in cyberspace, seen from a legal, ethical and societal perspective

In this chapter will try to answer sub question 6: What are the possibilities and constraints of enforcement in cyberspace, seen from a legal and ethical point of view?
We have now arrived at the empirical part of this research. That means the answers to these sub questions were based on the semi-structured expert interviews. Where it was relevant, the source of a statement was added. In some cases, for example when a certain article in the law was mentioned, articles of law or case law were added to enrich the analysis.

4.1 Legal perspective

In chapter 3 it was concluded that the police authority to use legitimate force could be translated to cyberspace. But what legal issues should be reckoned with? The first section contains some general points mentioned by the respondents, in the later sections some specific topics are discussed: the relations with the armed forces and specifics of The Onion Router (TOR).

First, the law: does it currently allow for enforcement in cyberspace? The law is always in development. Politicians change it, but it also develops by legal interpretation, by applying what judges think of something. What was theft was clear in former times: stealing things physically. That changed when the Internet came and we started to steal avatars[5]. Now there is case law about that: is this theft of a digital good? You can get money for avatars and virtual items at online marketplaces, so it is a 'good', as meant in the law. So the law develops itself. Nonetheless, a legal expert states that he can imagine that some judicial changes are needed to start using cyber enforcement methods. If the law now describes everything in such a way that it doesn't cover the Internet, something needs to be changed. For example by legally stretching the existing definitions or by saying that we make a separate category about cyberspace. If the police have the task to maintain law and order and they can use certain resources for that in the physical world, and none in the digital world, something is wrong.

However, the possibility to hack is already included in the proposed law on computer crime in the Netherlands. The 3rd law on computer crime contains new articles that enable the police to enter an automated work. More specifically, in case of a crime that allows for temporary custody, a suspicion of involvement in an organized criminal group, or indications for terrorism, *"the prosecutor can order an investigative officer to enter an automated work that is in use by the suspect, with or without a technical tool"* (Dutch Government, 2015a). So can the police use this law to hack systems and disrupt the criminal process? No, firstly the law has not yet come into force; As of 2016, it still needs to be approved by the Dutch House of Representatives (Staten Generaal). Secondly, This 3rd law on computer crime relates to powers of investigation, which are determined within the code of criminal procedure. The powers thus fall, like all special investigative powers, within the code of criminal procedure. Criminal

[5] A user's virtual representation in a computer game, a graphical object, which usually has a human-like form (Strikwerda, 2014, p. 7 & p. 24).

proceeding is about collecting evidence in the investigations for the prosecution of a person, so the proposed law is not meant for other law enforcement goals, such as disruption.

However, the explanatory memorandum of the proposed law contains an addition stating that entering an automated work (the hack) can also be used for disruption. An interviewed legal expert declares that he doesn't know what the lawmakers mean there, because criminal procedure is not primarily meant for disruption.

"At the time that you use an in instrument from criminal procedure purely for disruption, then as far as I am concerned you are guilty of 'detournement de pouvoir', a misuse of its powers, because you use an investigation instrument for a purpose other than what it was written for. And if the judge thinks the same, it leads to exclusion of proof or inadmissibility of the court. So you would need to arrange that in a different way." Legal expert

This legal expert is clear. If you already know upfront as prosecutor that you are not going to succeed in a case, and you just want to disrupt, then you cannot use an instrument from the code of criminal procedure for that single goal. Criminal proceeding is intended to gather evidence for a judge, who then decides what would be the correct punishment for the suspect, not for disruption of criminals. It is designed to create a process in which evidence is collected, and then there are also all of rules designed to ensure that this happens neatly, and then finally someone will be convicted when the public prosecutor decides to prosecute. Then the pieces of evidence are admitted, the defense can make a problem of that and the court can impose a certain conviction. The code of criminal procedure is fully rigged for streamlining that process.
However, he does declare that in some investigations, disruption is seen as a second objective. So first the aim is to gather evidence: who is behind the botnet, who connects with the server and can we find the identity of that person? And after that, the botnet could be used to perform disruptive actions and maintain public order, but as a second target. In the Descartes investigation in 2012, pictures on child pornography sites were replaced by police logos. The first objective was to identify the perpetrators for prosecution.

A respondent also mentioned an article that is in the law already, about (house) searches and police powers. Article 125j describes the so called "network search", which enables police to search a system that is in another location from the location that the search takes place at, provided that the people who live, work or reside at the search location, are granted access to such a computer with the rightful owner's consent (art. 125j Sv). There must be both an actual bond between the person and the location where that search takes place (not a network search from the smartphone of a casual visitor or cleaner), as a legal bond (agreement) between the person and the computer elsewhere (so no network search in computers that were hacked by the suspect)(Koops, 2014, p. 16). According to the respondent, the network search could be coupled to deleting data (art. 125o Sv), and therefore could be a potential enforcement method in cyberspace. In a very limited number of cases, in which a setup is found that meets the requirements of this law that is indeed possible.
But the method is not a serious contestant as enforcement method in cyberspace since it can only be used during a physical house search, vehicle search or search in a place other than a house, with strict conditions (the latter two require a crime in flagrante delicto, or a crime for which temporary custody is allowed)(Conings & Oerlemans, 2013). Hacking into the connected systems is not allowed, because there should be a legal bond with the other system. This, and the need of a physical address to start, which most crimes in cyberspace lack, make

the possibility to use it as an enforcement method in cyberspace very small. And apart from that, most importantly, the network search is part of the code of criminal procedure and is meant for collecting evidence for the prosecution of a person, not for other law enforcement goals such as disruption.

So if you want to use enforcement methods purely for disruption, this should be regulated elsewhere. A cybercrime expert has an interesting idea: using article 3 of the Police Law (enforcing law and order and helping those in need of assistance).

"The hack capability in the new law that will now possibly be implemented is clearly meant for criminal proceedings. I am very curious as to whether you also have the possibility to deploy it on the basis of Article 3 of the Police Law. But I suspect that this could become complicated." Cyber Crime expert

If you look at police enforcement in cyberspace from this perspective, this changes the dialogue. When performing disruptive activities, the police could say: we propose that, based on the protection of our people, without attempting to obtain information or whatever, but just to stop the offense, the police can use the following methods. This approach is similar to the cops on the street that stop a fight, or a thief running away after pickpocketing someone. There are a number of cases in which article 3 of the police law is used as justification for police actions. An old example is the so called "red flag arrest" from 1977. The case is about an action on the 1st of may in 1975, the Labor Day celebration. The Supreme Court approved the action of a police officer who, in order to maintain public order, took down and seized a red flag that was attached to the town hall. Carrying out article 3 of the Police Law (in that time article 28 of the Police Law) was seen as sufficient justification for the action. The action was explained as a *"police measure in the interest of maintaining public order",* and deemed suitable because it was *"required in the situation according to reasonable insights, and the measure was in proportion with the degree of public disorder"* (Supreme Court, 22 February 1977, NJ 1977/288). Another example is a more recent case from 2009, in which a police officer opens a car door to see what the driver is doing with his hands. At that moment the driver throws a packet of drugs on the car floor. The court approves the action of the officer, stating he used article 3 of the Police Law (in that time article 2 of the Police Law) justly to open the car door on the basis of suspicious behavior (Court of justice Leeuwarden, 5-8-2009, ECLI:NL:GHLEE:2009:BJ4666). A third example is a case from 2013, in which a person in a mentally confused state was screaming on the street that he would set fire to everything and stab everyone. Police officers arrested the person on the basis of article 3 of the Police Law (Court of Limburg, 20-3-2013, ECLI:NL:RBLIM:2013:BZ5447).
The example cases show that there are various actions that police officers can perform on the basis of article 3 of the Police Law. However, they are all in the physical domain. What will be seen as proportionate measures in relation to the degree of public disorder, or the degree of the criminal offenses in cyberspace is still a question mark.

"It's about stopping criminal activities. Imagine, someone aims a water cannon on something, and you cut the hose that supplies water from the ditch. Cutting the hose seems aggressive, but in fact it is simply the stopping of criminal activities. Why would you need a new legal basis for this? The police are very clearly limited when it comes to the infringement of your privacy as a citizen. But at the moment they see drug trafficking in the physical world, they may simply disturb and stop this. Why wouldn't it be the same in cyberspace, and who will accuse you?" Cyber Crime expert

Hacking with the aim of investigation and bringing people to court is an infringement of privacy and needs permission to ensure that it happens proportionately and legitimately. But hacking could also be used to stop crimes, without prosecution and a lesser infringement of privacy. It is a different objective: purely for something to be stopped. According to the cybercrime expert, this is already possible without need of a new legal basis, if you do things transparent and explain why you do it. He adds that, when the target you hack is in another country, you should also ensure that the public prosecutor within the jurisdiction agrees with the action, otherwise your action is unlawful.
A legal expert does not agree with this. He explains that not everything can be done under the general article 3 from the police law, when there is more than a minor infringement of the basic rights of the person concerned, e.g. the right of privacy, a legal basis is needed. This derives from the Zwolsman-judgment and is based on the legality principle[6].
Some enforcement methods in cyberspace will be under that threshold and some will be above. The legal expert argues that it would be good to change the Police Law for this, to have a legal basis:

"I am thinking of the Police Law. That you add it to the existing, classical, enforcement methods, on the basis of the article that indicates that the police may use force. Apart from that you have the official instruction in which the instruments/weapons are summed up and the conditions under which they may be used. In the explanatory memorandum or in case law by judges, the digital enforcement method could be defined. You should continue to reflect on this: do my instruments still fit these phenomena? You could even say: we just use this once, and then we look at what happens in court. But I think you must take your responsibility as legislator and propose an amendment." Legal expert

When actions are only meant to disrupt, there are other legal consequences as well. You need to make up rules about what you are going to do with the information that was found: how do you delete it and how do you make sure it is not used for prosecution? Apart from that, a digital civil rights expert argues that when the police make a site unreachable, the site owners should have the possibility of redress. In theory they should have the possibility to organize a defense. The likelihood that they will do that is small, but there should be a possibility. So if a hack (in case of disruption, not investigation) is performed by the police, the site owner/administrator must be informed that it was the police that hacked the website.
In line with that, is the distinction whether an action is permanent or not. After a hack you could delete and destroy data. That would be a more thorough action than a (D)DoS attack, that only makes data temporarily unavailable. The distinction between permanent or temporary should be taken into consideration when determining the impact of a method.
You also need to think about is what will happen if things go wrong. If for example you take the wrong website offline, that could have considerable legal and financial consequences. These are things you need to think about before you start these actions.
Finally, there is the challenge of the international nature of cyberspace combined with sovereignty and jurisdictions. A large portion of cybercrime comes from abroad; therefore the police should have a clear idea

[6] The principle that government actions have a basis in the law and are carried out in accordance with that legal basis (Voermans, 2011, p. 8).

how to deal with the sovereignty of other states when considering cyber enforcement methods. In some cases, if political leaders approve it, it is possible to violate the territorial sovereignty of a state willingly. Imagine that a large number of companies and citizens are victims of a great deal of financial crime and all types of malware, and everything comes from one country that does not respond to legal requests at all. Then the police would be able to start a judicial investigation or disruptive activities. It will be in conflict with the territorial sovereignty and with international law, but that could be a choice. Will you start an international conflict because of a piece of child pornography on a server, continuous DDoS attack waves, or theft of critical business information? That is a political issue as well.

Relation with armed forces

It is not always immediately clear who is responsible to act upon criminal conduct in cyberspace. It is possible that an event is seen as an offense to be handled by police first, but later also comes to the attention of the Department of Defense. A security breach in a system can develop as multiple affairs in several areas of policy, appearing on the agenda for police, intelligence service and armed forces. There are organizations in the Netherlands, the NCTV (National Coordinator Anti-Terrorism and Security) and NCSC (National Cyber Security Center) that coordinate the responses to an incident.

The police are most often the first government agency to act when cybercrime takes place. In some cases it is possible that a cyber incident is not only a crime but also a threat to national security. Then the armed forces could take over. If someone broke into the department of public works (Dutch: Rijkswaterstaat), and manages to take down all the water defenses and all dike rings in the Netherlands at the same time, then you would have a situation that could result in thousands or even a million deaths. In that case there is a situation in which the government can say that they feel attacked as a country and get the armed forces ready to respond. If the intelligence services have the capabilities, they can also do it, and if the police can do it, they may as well. These two are preferable before the armed forces move. However, the police do not have the tools yet. If enforcement methods in cyberspace will lawfully be added to their equipment, they could enter an automated work and eliminate a source. But where exactly does the role of the police end and where does the role of intelligence agencies and armed forces start? Future research can give more insight into these matters to some height.

The Onion Router (TOR)

One of the respondents compared TOR hidden services with ships performing criminal activities on the open sea. To act against crimes on the open sea, the United Nations Convention on the Law of the Sea (UNCLOS) was written. The UNCLOS is possible for piracy on sea because it is a universal crime[7]. Trade in hard drugs, which is done a lot on TOR hidden services, is not a universal offense; it is simply a crime in all countries separately. What is prohibited in one country is not prohibited in another country; this also goes for drug trafficking. A legal expert states that a sort of law of the sea is not applicable to TOR. He refers to a WODC (Wetenschappelijk Onderzoek- en Documentatie Centrum, Scientific Research and Documentation Centre)

7 *"any conduct which manifestly violates a fundamental universal value or interest, is universally regarded as punishable due to its gravity, and is usually committed, organised, or tolerated by powerful actors, and which therefore may require prosecution before international courts"* (Einarsen, 2012, p. 298).

report on cross border investigations in cyberspace and states that TOR is no sea. There is not really a part that belongs to no one, as there is always a link to a jurisdiction. So you always come in a jurisdiction of another State, more than you do on the sea. States could propose certain measures, for example an agreement with a number of states that says: when these kinds of drugs are traded, you can take a site offline. But nothing keeps the Dutch police from doing something already. So then you say: the States may not happen to make an agreement with each other to specify the conditions under which an action is allowed, but they can write policy for themselves. According to a legal expert several countries already follow the principle that when people use TOR/VPN and their location cannot be determined, law enforcement just acts across the border.
There are situations in which several jurisdictions apply on the same phenomenon. If there is a Dutch connection, e.g. the suspect is a Dutchman, or you bring the drugs to the Netherlands, a Dutch prosecutor can also claim jurisdiction. So if there is jurisdiction is and there is a punishable crime, prosecution is possible. This doesn't need to be a universal crime.
So if there is a connection somehow with the Netherlands, a prosecutor could claim jurisdiction and take action. But in the first phase you usually have no idea where things are located, and the jurisdiction is not known yet. And only after you hack the website you can see the location. If it is going to the United States for example, you could say, I will now get in contact and continue with the FBI. This is also how the proposed cybercrime law in the Netherlands describes this issue. If you cannot find a location, then you can take a first action (Dutch Government, 2015b, pp. 51-54).

4.2 Ethical and societal perspective

Cyber enforcement methods can also be described from an ethical and societal perspective. Off course, some methods to enforce the law will be technologically and legally possible, but police work also has an ethical element. How will the enforcement methods in cyberspace they affect our daily lives, will they change society, is the end result desirable?
First of all, there will always be people unhappy with some enforcement methods. Just as unhappy as when the riot police clean a square of protestors. Some actions will not make you popular, but they need to be done. And maybe that's the same in cyberspace. If everyone, including criminals, explores and discovers his or her digital identity, why wouldn't the police do that as well? They have to find their way, and sometimes that will include trial and error. That does not mean that they can simply do everything that they also in do the physical world. We will now look at a quote from a cyber security expert, quite comprehensive, but beautifully and clearly explained:

"The question is: how far should you go as police? What freedoms do you think you can take away from people in order to take certain measures? You can perform a digital break-in, you can turn something off or take it over. You can do all that. But then you need the authorization to do so, just as you need a search warrant in the physical world. It must be justified. You cannot just say: we make a police state of it, where the police suddenly have more digital powers than in normal life. The opposite is more probable: that you should fight for the equivalents of the powers you have as police in physical life, and sometimes other, new opportunities will arise, which are not exact analogies. That police state feeling is much stronger on the Internet than in the normal world, because in the normal world we have had the police already for a few hundred years. There were some peaks when we thought: this is too much, we really don't want this no more, and we have had periods that it was too low, when we wanted more security. Now we have a kind of

balance and we constantly tinker with it, it always moves a bit. In the digital world it will be the same. It may be that you now say: Well that is a pretty nice method. But the world could change which can make the method much more radical. Or the other way around: you now think that a method is very intrusive but that it will be totally normal in the future." Cyber Security Expert

The above quote is a very good description of the situation we are in. This respondent realizes that we should constantly think about the methods that are used and their impact on ever-changing society. A good example to illustrate this idea: we are on the eve of the self-driving car age. These cars will bring a lot of opportunities, but dilemmas as well. As the respondent said, you can do a lot as police, but where is the balance? Maybe it will be technologically possible to hack the car of a dangerous suspect, and let the car drive to the police station for an interrogation, instead of trying to arrest him, spending valuable manpower. This sounds far-fetched and crazy now, but maybe it will be normal in 20 years. For now, it would be good to clearly state in the law what can and what cannot be hacked, to prevent a situation of, as the cyber security expert describes, "too much police state".

A digital civil rights expert adds that the discussion about how and when these kinds of methods should be deployed is extremely important. An example: the freedom of speech should not be harmed. All the cases in which there is disruption without assessment by the court and without the possibility for the subject to defend himself, can cause the freedom of speech to be harmed. The expert states that if the police would systematically disrupt certain type of forums then you can no longer express a certain opinion, and that would be a problem.

"We always look in particular at the freedom of speech and privacy. What is being proposed and is it necessary? It has to be a balance of proportionality and subsidiarity: what is its purpose, is there a need for it, what is the further impact, are there disadvantages? Is everything balanced and do those powers in general weigh up to the infringement they cause, do these methods actually resolve the problems or may there be a different way? For all these methods, all these questions must be answered before they are approved. And then, after implementation, each individual case should be assessed. So first a general assessment, then an individual assessment." Digital civil rights expert

Some respondents point out that enforcement should happen in transparency, with police saying: from now on, we will use these methods, and if something goes wrong here we will deal with that transparently. The police must always be able to explain it. And they also need be fair to say that it is all new, there will be borderline cases in which the court should decide whether something is justified or not. This creates a system of subsidiarity and proportionality.

A digital civil rights expert warns against the risk of the sliding scale: when police get used to these methods, they could start using it for more and more types of websites. In the beginning, deployment could be very strict, but the judgment could "slide" to the other side. And that means, as stated before, that you need to determine what can and what cannot be targeted.

A legal expert points out that in some cases, for example when the democratic order is in jeopardy, the AIVD (General Intelligence and Security Service) could also perform enforcement actions in cyberspace. But the question is, is it desirable to let such an agency perform these tasks? The doings of such an organization are shrouded in mysteries and performed secretly. Maybe, when looking at the current sentiment in society, e.g. the

Snowden case, it is a better choice to equip the police with the necessary tools to do these things transparently. The police task includes stopping criminal acts, so equipping the police to do so in cyberspace is in accordance with that.

4.3 Pre-conclusion

Some methods will be technologically feasible, but the police should always do things lawfully and ethically. Therefore this in depth analysis into legal, ethical and societal perspectives was conducted. The respondents brought up a great number of issues and themes that should be thought of when considering the use of enforcement methods in cyberspace. This urged us to make a selection of the most significant issues.

Although the authority to hack is introduced in the proposed 3rd law on computer crime that does not mean that the method can be used for purely disruptive purposes. The law on computer crime is in the code of criminal procedure, and ultimately meant for the prosecution of a person. Disruption can be a second goal in addition to prosecution, but not a first. To use the hack for disruption of criminal processes, another legal foundation is needed. This is probably the same for other enforcement methods, but opinions about the legal foundations that are needed differ. Some respondents believe that the existing article 3 from the Dutch Police Law is enough justification to use these methods, whereas others think some adjustments in law are needed. It will probably depend whether or not the method causes more than a minor infringement of the basic rights of the person, the legality principle. Because this is important for further decision-making, "privacy intrusion" and "violation of free speech" will be included as attributes to classify the enforcement methods in chapter 5.
The most probable place in the law for the cyber enforcement methods will be the Police Law and the Official instructions for police, royal constabulary and other investigation officers. An alternative strategy is also mentioned: just using a new method once and then see what judges will say about it.

The international aspect of cybercrime is also a legal challenge. Since a large portion of cybercrime comes from abroad, there is a big chance you violate sovereignty and jurisdictions of other states when using an enforcement method. If there is somehow a connection with the Netherlands, a prosecutor could claim jurisdiction and take action. This is the same for the TOR web. But there is a difference, because on TOR you initially have no idea where hidden services are located, so the jurisdiction is unknown. Only after you hack the website the location becomes visible. The proposed cybercrime law in the Netherlands describes this issue as follows: if you cannot find a location, then you can take a first action.

In the second section, some ethical and societal issues were discussed. An important realization is that we are just starting to explore enforcement in cyberspace. We should constantly think about the impact these methods have on the ever-changing society, e.g. what freedoms can be taken in order to take certain measures. Just as happened with enforcement in the physical world, the police needs to find a kind of balance. This balance will be constantly tinkered with, it always moves a bit. To let this process run smoothly, the enforcement methods should be used transparently and the police must be able to give explanation.

Respondents also warn that extra caution is needed when certain enforcement methods might bring freedom of speech at risk. If the police systematically disrupted certain types of forums, citizens could no longer express a certain opinion, and that would be a problem.

A major consideration is the potential loss of trust that people have in the Internet. The Internet, for example BGP routing, functions on the basis of trust. Certain enforcement methods could have a negative influence on that.

5. Potential enforcement methods in cyberspace

The preceding chapters looked into the importance of cyberspace and concluded that the police authority to use legitimate force can also be applied to cyberspace. The question that follows, answered in section 5.1, is sub-question 7: When and how should police, considering the principles of subsidiarity and proportionality, use cyber enforcement methods?
Sections 5.2 and 5.3 will answer the final research question: what are potential enforcement methods in cyberspace, and what are their characteristics?

5.1 How and when to use: proportionality, subsidiarity and other considerations

To answer the question how and when an enforcement method should be used by a police officer, the two most important concepts are proportionality and subsidiarity. Proportionality means that the amount or type of force that is applied should be proportional in risk and effects considering the intended purpose. Subsidiarity means that there should not be less intrusive options to reach the intended purpose (Naeyé, 2005).
Police officers strive to limit damage to others. If we make a comparison with the physical world: pepper spray may not be used in groups, because it is badly controllable: it can go everywhere. That type of instructions could also be composed for the use of force in cyberspace. If officers could use all enforcement methods freely, without rules and restrictions, it could result in damage to innocent digital bystanders. So these concepts also apply to enforcement in cyberspace. Therefore collateral damage and predictability will be included as attributes to classify the enforcement methods.

"Normally if the police use force, they have had a lot of instructions before they may draw a firearm, and they must report all use of force. And if there is a chance that they hit bystanders they may not shoot. These kind of things should also be sorted out here." Cyber Security Expert

The subsidiarity principle is concerned with the question: is this the way to do this or would it have been better and easier to simply ring the bell, in case we know where the suspect resides? Almost all respondents indicated that it is more interesting in the Netherlands to just get the car and drive to the suspect. But as described in chapter 2, the physical location of the perpetrator is mostly unknown. A digital enforcement method could also be interesting when a physical action costs far more time and money, and leads to the same end result. Some respondents were not entirely convinced by this, they prefer the physical approach when possible.
These respondents also mentioned a risk: a future where the police use force in cyberspace too quickly. As example they mention the recent takedown of a website for a squatter party on Queens day. The site displayed former Dutch queen Beatrix with a rope around her neck. The Internet service provider took down the whole webserver after a request from the police. So not only the page was made inaccessible but the entire website, plus hundreds of other websites that were hosted on the server. The respondents fear that force in cyberspace will be used for similar goals when the police acquire more options to use it.

Although collateral damage must be limited, sometimes it cannot be avoided. A respondent explains this and refers to the physical world:

"If the riot police roams through a city they also close streets and there is also collateral damage. Once, a bike of mine was broken because the riot police wanted to jump on a wall and stepped on my bike first. They just jumped on my bike, a frail bike, and it snapped. I never got a new one." Cyber Security Expert

Finally the physical world and the digital world will mingle with each other when choosing a suitable use of force:

"When you look at the concepts of proportionality and subsidiarity, the digital and physical worlds are already mixing. There may be situations in which first a physical approach is the best choice, then a digital approach, and then a physical approach again. You should not completely separate them, it should be considered as a whole: will we take this digital or this physical method?" Cyber Security Expert

You should also make protocols that describe how to use the enforcement methods, similar to existing protocols for the use of physical weapons. These could contain conditions and explanations, for example that a server can also be a shared hosting unit with numerous websites.

When the use of cyber enforcement is considered, there is also a risk of counterattacks against the police. Targets of police enforcement actions could try to hack or (D)DoS the police, out of revenge. The extra risks this poses for the cyber security of police infrastructures should be considered. It will depend on the targets that are chosen: child pornography websites would probably pose little retaliation risk, but for dark net markets this is already less certain. Hacktivist groups such as Anonymous are known for cyber attacks against institutions that antagonized them or that act in conflict with their philosophy (Coleman, 2014).

5.2 Potential enforcement methods in cyberspace and characteristics

The list of methods that are deemed potential enforcement methods in cyberspace was composed using the interview results. The methods in the list will be described and classified by means of a number of attributes. The first attributes were derived from literature, and these were complemented with attributes distinguished during axial coding of the interviews. The attributes are:

Proportionality		*Legality*		*Legitimacy*	*Practical usability*	
Collateral Damage	Predict-ability	Privacy Intrusion	Violation Freedom of speech	Reliance on third parties	Feasibility	Effectiveness

Proportionality	- Collateral damage: the number of bystanders that suffer damage as consequence of the action and the amount of this damage. - Predictability: the possibility to predict the results of the action prior to execution.

Legality	- Privacy intrusion: the degree to which the right of privacy of the target is impaired. - Violation freedom of speech: the degree to which the right of free speech of the target is impaired.

Legitimacy	- Reliance on third parties: the degree to which the police depends on third parties for deploying the enforcement method.

Practical usability	- Feasibility: The degree to which the action can be easily executed. - Effectiveness: The degree to which the action is successful in producing the desired result.

The following symbols will be used to classify the methods:

- : The method scores bad

+ : The method scores good

+/- : The method scores intermediate/indecisive

The process was iterative: the list was fine-tuned constantly, some methods were added and some were discarded. To be included in the list, a method should meet the following requirements:

1. It should be, up to a certain extent, a *proportional* method: collateral damage and predictability should be reasonable.
2. It should be a *legitimate* police enforcement method, deployed by the police and not a third party.
3. The method should be *practically usable*: execution should be feasible and effective
4. The method must be usable for enforcement and disruption, not only for investigation.
5. It should be a pro-active/reactive method, not a preventive method.

The discarded methods are listed at the end of the chapter.

5.2.1 (D)DoS attack

The essential characteristics of the (D)DoS attack were already explained in chapter 2, but now we will to look at the it from another perspective: the (D)DoS not as a criminal but as a police instrument. This requires a mind shift: DDoS services are now completely illegal, but the same counts for physical violence weapons such as a gun. Guns are illegal in the Netherlands, but not for the police, they can buy it from a legitimate reseller.

"And here comes the challenge, someone will need to build a legal DDoS service, but that will only become legal, if the police would rent it and in addition would get the judicial possibilities to use it. So it is a chicken and egg situation." Cyber Crime expert

As possible targets of a (D)DoS attack, the following layers can be distinguished: first the network layer, then the operating system layer, and on top the application layer. Another model to make a classification is the "LAMP". That stands for the frequently used software Linux, Apache, MySQL and PHP. PHP is the programming language to make websites, MySQL is the database, Apache is the webserver, and Linux is the operating system. Each of these letters is a layer that can be attacked. If you just perform a raw (D)DoS attack with a lot of traffic, the network interface of the server will be flooded: a low layer. The operating system doesn't notice that. The application that you want to take down in the end, a website, doesn't notice it either. But the site is unreachable, because there is simply not enough bandwidth available to meet the requests.
Some people find the (D)DoS an atrocious action. An Internet infrastructure expert gives the following description: "(D)DoS as an instrument to tackle one specific site is similar to a scenario in which drugs are sold in a city and you throw an atomic bomb on it to ensure that nobody deals drugs anymore". According to him it is an extreme instrument that leads to victims and high costs for another party: the hosting provider. This provider could host ten thousand other sites that could be taken offline as well, a lot of collateral damage. This criticism relates to (D)DoS attacks on the network layer that send large quantities of traffic over services and connections.
But besides such "brute force" (D)DoS attacks with a lot of traffic, there is another option: a much more targeted attack on a higher layer. In that case you do not necessarily have to send a lot of data, so you can restrict collateral damage.

"Let's say that the target website is a forum which contains a search field. If the website has to look through all posts, then it must do a lot more work than when it only needs to cough up the first index page, which may well just be cached somewhere. So what you could do is constantly adding new searches to construct a DoS attack." Cyber Crime expert

The above attack on a high layer may be interesting for the police because they prefer as little collateral damage as possible. Oppositely argued: perhaps these attacks can also be mitigated more easily with firewalls and other kinds of defense. Anyway, the respondents all agreed that successful (D)DoS attacks are possible without sending extreme traffic volumes.

"I think you can paralyze a lot of servers when you have a gigabit connection. Sometimes we also do (D)DoS testing here, when customers ask us whether we can take something out of the air. Mostly we can with only one laptop, it's really scandalous how easy it is. But these are intelligent DoS attacks, on a higher layer. So not just sending many packets, but for example continuously repeating the authentication login. And that can also be used in the event of a Command & Control server, because then you just pretend to be a

little bot and completely fill the server with data. And if they find out they probably filter your IP address, but then you simply attack from a different IP address. And then it is ultimately something that you can do for a few hours before you can eventually go into that bunker." Cyber Security Expert

The (D)DoS could, due to its temporary effect, be a useful method in the first phase of a police intervention to attack the system or website, before further measures such as a seizure may take place.
To perform DDoS attacks, an infrastructure with a good Internet connectivity is needed to produce enough traffic. Maybe you want to attack multiple targets at the time, so capacity is needed as well. It's possible to build an infrastructure for a botnet, but that requires connections in many different places, maybe servers abroad. The latter can be legally difficult; possibly you violate sovereignty of the countries where those servers are located. Therefore, a cybercrime expert points out it would be easier to keep the botnet within the Netherlands. What could be another option is a joint initiative between some countries. If law enforcement agencies create a botnet together, it would already be harder to block than a botnet from one country. Another cyber security expert agrees that it would be a challenge to do the attack from one location, since it is easier to block. He advises to use at least multiple locations in the Netherlands. Off course, the target could say: I block everything from the Netherlands. But if most of his visitors come from the Netherlands, this is not an option.
And how about the equipment? (Designated) personal computers in government buildings could be used for a (D)DoS. That is quite easy to do. You could also use a very powerful DOS generator in a datacenter, but that is easily identifiable. Within a short time it will be known and filtered out by the community. So, once again, it's better to distribute it as widely as possible.

A cybercrime expert does not see ethical problems when the police builds a botnet to perform (D)DoS attacks, if it is used sensibly. The moment you paralyze a darknet market, you disrupt people who are doing something illegal. According to the expert this will probably be the same from the UN perspective: at the moment that an illegal marketplace is blocked, no one will have a problem with that.
Amplification is something else: it is technically possible for the police to use DNS amplification when performing a (D)DoS attack, but respondents say it would be morally despicable because you use infrastructure of an unsuspecting third in order to achieve your goals. In addition, it is possible that the DNS server tips over, due to overuse. The experts have different thoughts about the legality of DNS amplification, but ethically they all condemn it.
When a botnet is rented from a private party that would be a new situation: never before did the police need a private company to use an enforcement method.

"The police has its own weapons and its own riot police, and if you would now say: you require a private party to do this, it will start a discussion such as the one between Apple and the FBI about encryption. Those tech companies simply don't want to be an extension of the police." Cyber Security Expert

Properties of the (D)DoS attack

What is crucial with regard to collateral damage is whether a (D)DoS attack is on a high or a low "layer": attacks on lower layers cause collateral damage, because it could also take other sections of the provider network offline. Suppose that the server that will be attacked is a shared server, that hosts three hundred websites, and one of

them is bad, then an attack on the network layer of the server is much heavier than if you can only target the bad website via the application layer.
The predictability of a (D)DoS attack is poor, especially on a low layer. A cyber security expert indicates that the effects cannot be estimated. You can have a specific indication, you can assess the route to a server, but you never know for sure. During a (D)DoS attack, the infrastructure observes pressure on a certain line, and looks for an alternative route for the traffic. You can never say in advance what route the Internet traffic is going to take. So you can never be sure that you are not causing collateral damage. That is difficult because the police are often looking for certainty. But here as well, attacks on a higher layer are easier to predict since there are fewer alternatives available. Because the low layer (D)DoS causes collateral damage and is unpredictable, it is discarded as potential cyber enforcement method.
In the event of a (D)DoS attack you generally stay outside the system, as opposed to a hack. Therefore the (D)DoS is an alternative with less privacy intrusion. Whether freedom of speech is violated depends on the target of the (D)DoS.
According to a cyber security expert, setting up a police botnet is not a problem, so there is no reliance on third parties:

"Setting up a botnet yourself can be fairly simple. It will not cost a lot of money either. If you look at those DDoS guys, they mostly don't have more than 20 to 200 servers in their botnet. That is not very much. And they get every website offline with that. Off course, you cannot get the larger websites offline but that I think that shouldn't be the goal of this tool anyway." Cyber Security Expert

With regard to the effectiveness of the (D)DoS one must take into account the temporary nature. An attack can continue for some time, but is ultimately temporal. Therefore it is a limited tool in this sense. But in some cases this is precisely the intention.

"Suppose that the server is somewhere in a bunker or something alike, the hoster does not respond, and hacking takes too long, then I think that you should indeed stuff it full from a certain pipe." Cyber Security Expert

An Internet infrastructure expert has his doubts about the technical effectiveness of the police DDoS. He thinks that it is very easy to mitigate because websites simply get a Cloudflare account: they pay anonymously with a stolen credit card, swipe the card and get their protection. Cloudflare is a company providing website acceleration and a DDoS protection service. If "bad" websites indeed all get such an account, this could be a reason to cooperate with this company as law enforcement sector. On the other hand, it is unclear whether the Cloudflare service also protects website against "smart" (D)DoS attacks on a high layer.

	Proportionality		*Legality*		*Legitimacy*	*Practical usability*	
	Collateral Damage	Predict-ability	Privacy Intrusion	Violation freedom of speech	Reliance on third parties	Feasi-bility	Effective-ness
(d)DoS attack (high layer)	+	+/-	+	Depends on case	+	+/-	+/-
(d)DoS attack (low layer)*	-	-	+	Depends on case	+	+/-	+/-

* Discarded

Table 1: Properties of the (D)DoS attack

5.2.2 Internet shutdown

A potential enforcement method mentioned by several respondents is shutting a district, a street or a building off from the Internet. If the police can physically block buildings and streets, why wouldn't they also block the Internet?

This concerns both the Internet via air interfaces (e.g. UMTS) as via cable connections. Internet via air interfaces could be disrupted, for example with jammers to scramble the signals. This is possible because both UMTS as WIFI work on a modest number of frequencies. In the event of UMTS you do have the risk that you also disconnect all other users in the vicinity. Wired Internet connections, for example directly via a router with a cable that goes into the ground, are a different story. In that case you need the help of the provider.

Properties of the Internet shutdown

Shutting down the Internet can be done in many ways, which makes it difficult to specify the method.

First of all there is the distinction between Internet via air interfaces and Internet via cables under the ground. Secondly there is the distinction between application on a small scale (apartment) and on a large scale (city). For that reason the characteristics of the Internet shutdown differ when it concerns for example collateral damage.

Digital civil rights experts indicate that they find the method disproportionate in most cases, for example during riots. Their motivation: you disconnect an essential means of communication of many people, when only a few people abuse that medium. But they also declare that some situations are an exception, for example when there is a hostage situation and armed men hold people at gunpoint. In that case they can imagine that a judge allows it.

The results of the Internet shutdown can be predicted in advance, signal jammers can be programmed for a certain range and when shutting down cable, the houses or streets can be selected.

Privacy intrusion of this method is severe: you take away an essential means of communication. There is also a violation of free speech: without an Internet connection it is almost impossible nowadays to express yourself.

Lastly, in case of a cable connection, the police rely on cable providers: they cannot independently shut down a location from the Internet. That makes it less a "police" use of force, for that reason the internet shutdown of cable connection is discarded as potential enforcement method.

	Proportionality		*Legality*		*Legitimacy*	*Practical usability*	
	Collateral Damage	Predict-ability	Privacy Intrusion	Violation Freedom of speech	Reliance on third parties	Feasi-bility	Effective-ness
Internet shutdown (UMTS/WiFi)	Varies	+	-	-	+	+	+
Internet shutdown (Cable)*	Varies	+	-	-	-	+/-	+

* discarded

Table 2: Properties of the Internet shutdown

5.2.3 Hack & shutdown/encrypt/destroy

Suppose there is a criminal website or Internet service that you want offline, and the provider does not cooperate. In that case you could hack the network to take it down from the inside. Hacking is a wider concept, but in this case the hack is defined as follows: “entering a computer system without physical access to it and without permission from the owner”. When you have hacked a system you can for example delete data and wipe hard drives.

To get into a system, you need to find vulnerabilities that can be exploited. In literature and media a lot is written about so-called "zero day exploits/zero day vulnerabilities". These are vulnerabilities in software that have not yet been publicly announced. There is almost no protection against these "zero days". The software cannot be patched yet and anti-virus products do not detect the attack (Bilge & Dumitras, 2012, p. 1). Zero days are expensive and rare, but they can be bought legally. An example: the American National Security Agency (NSA) spent 25,1 million dollars on zero days in 2013 (Fidler, 2015, p. 406). The use of zero days is seen as questionable: buying them and keeping them concealed worsens the cyber security in general.
Basically, the police would not need to possess and use zero days. However, some respondents do suggest that they could be used as a last resort in exceptional situations. A cyber security expert compares the use of zero days with the deployment of the special interventions team (anti terrorism unit) of the police. To deploy this team with their heavy equipment and weapons, the minister must give permission. You could place the use of zero days in the same setting, to insure political responsibility. Another possible option, for example when the police do not have a zero day and the armed forces of the Netherlands do (they don’t publicly reveal whether this is the case) is military assistance. If the police lack the knowledge, and the armed forces do have it, they can provide military assistance. The same applies for the Dutch Intelligence Agency, the AIVD.

However, the respondents in this research state that successful hacking is possible without zero days. One could use open source vulnerability scanners that use known leaks and known vulnerabilities to find holes in the defense.

"For example, you have a framework called Metasploit, that is simply open source, free to download, and it contains a shitload of different vulnerabilities. So that is just there." Cyber Crime expert

In many cases with simple crime, you could use the "simple" Metasploit tools to see if you can hack your target. Probably that works. The respondents expect a high success rate.

"You can hack perfectly without possessing zero day exploits. I think that you can have a success rate of 90% without zero days." Cyber Security Expert

According to respondents, a major technological challenge is the enormous variation in systems and potential targets to be hacked, and subsequently the required variation to hack these. Ready-made hacking tools are available on the market, but these will not always work. These tools will always use a specific weakness in the system that you attack, and if that is not available, or if it doesn’t work for another reason (e.g. the system is patched), the tools that you have on board are probably not working on the situation you encounter. A

cybercrime expert thinks it is more plausible that the police use standard tools for the moment they are already inside the system (e.g. to wipe hard drives, wiretap or create logs) than to actually grant access to the system.

A cyber security expert indicates that a hack probably works when the target is a larger infrastructure, e.g. a company network, because there is always someone that clicks on a phishing mail. If the target is one specific phone, it depends on the type of the product. A slightly older Android phone can be hacked, but if you want to hack the latest iphone with the newest iOS (Apple's Operating System) you almost certainly need a zero day. Respondents do not entirely agree on the question what is easier to hack: a telephone or a personal computer. As said, older telephone types are easier to hack than new types. It also depends on the number of apps on a telephone: the more apps, the more potential vulnerabilities. For personal computers, criminals already built many attacks. There is more knowledge about hacking a Windows computer than about hacking a telephone. So determining how easy it is to hack a system also depends on the amount of work others have already done.
In addition to technical tools, hackers also use social hacking/social engineering. They often start with that, for example by sending someone from the customer service a phishing mail to get access. Sometimes they even get in with only some small talk. This strategy could also be used against criminals. If you have a few days time you have a large chance to succeed. It might be a slow method but very precise. You must do it step by step and mostly the target needs to make a mistake.

"What hackers in the criminal circuit can do, bona fide hackers can do as well, there is almost no company network they cannot enter." Internet infrastructure expert

In addition to taking down a system by deleting information, there is also another way to take down a system: hacking a system and then locking the data on it by using encryption. Only the private key of the police could unlock the files. This method is already used by criminals and is known under the name "cryptoware". But you could also make it a legal police enforcement method. It would be a sort of digital equivalent of the handcuffs. Because you do not delete the data but encrypt it, you can decrypt it later for research, or simply to give it back to the owner after an investigation.

"But if we compare everything I think the combination of hacking and encrypting results in the most targeted way to digitally eliminate a crook, without disturbing a whole district or an entire network." Internet infrastructure expert

As was discussed in section 4.1, there is a proposed new computer crime law in the Netherlands that includes the authority to enter an automated work, in other words, hack a system during a criminal investigation.
It became clear that this law cannot be used for solely disruption, so another legal basis is needed. The requirements to use the hack for investigation are very strict, it can only be used for severe crimes. The question is: will this be the same when the hack is only used for disruption, and no information whatsoever is copied or looked at? When asked what is more intrusive, a digital civil rights experts explains that the disruptive hack is still an intrusion, a privacy violation, but to a lesser extent. The question for lawmakers is now: will it be possible to deploy this method for crimes less severe than is required for the investigative hack?

In the end, the discussion about zero day vulnerabilities is also an ethical one. If, in a hypothetical situation, the police could use zero days, the experts say the use should be limited to a maximum of 5 cases a year. These

should then be the most significant, severe cases. The impact of the case on the society must be so high that it's worth using such a radical method. This could be a case against child pornography kingpins, or organized crime groups that only operate through the Internet. It would also have to be the cases in which the Dutch citizen would like to see the suspects arrested. And the police should communicate it openly when this is used.

"If they can use it to tackle the big boys, and support this with a good explanation, they will get the respect of the public. But you should not use it against a cannabis grower. I think that will turn the public against you." Cyber Security Expert

Properties of the hack

According to experts that have experience with hacking the amount of collateral damage caused by a hack is small: because you really focus on a single system you will basically do no collateral damage. The same applies to predictability: trained and experienced hackers know what they're doing and the end result is fairly predictable: they will or will not gain access to the target system.

The majority of respondents indicate that the hack is a substantial intrusion of privacy. A digital civil rights expert states that a hack, whatever the next step is, will always be intrusive because you obtain access to someone else's system. The proposed law in the Netherlands, which enables the hacking and entering of computers, describes a hack as a very far-reaching instrument. It can only be deployed for severe crimes, probably with sentences of minimally six years or more. And even then maybe a selection of crimes. This will make it a challenge if you'd like to use the hack for disruptive activities in the future. But it also depends on what you do afterwards to determine how intrusive the method is. When you don't look at any files and only switch something off, the privacy violation is obviously smaller than when the hack is used to search all data on the system for a criminal investigation. And if you use the hack to temporarily turn off something, it is less intrusive than when you wipe the entire hard disk.
Whether the freedom of speech is violated depends on the target: when a political forum is hacked the freedom of speech can be severely violated. When a command and control server that sends out orders to zombies in a criminal botnet is hacked, or when a TOR hidden service where that sells credit card dumps is hacked, it is a different story.
There is not a reliance on third parties: according to the respondents, police hackers could perform the hack without needing others.
The hack is seen as highly effective. After a successful hack you could delete data and wipe hard drives. That is rather definitive, rendering the website longer inaccessible than when a process is only shut down. Off course, the target could have back ups that can replace the deleted files, but that is not guaranteed.

	Proportionality		*Legality*		*Legitimacy*	*Practical usability*	
	Collateral Damage	Predict-ability	Privacy Intrusion	Violation Freedom of speech	Reliance on third parties	Feasi-bility	Effective-ness
Hack & shutdown	+	+	-	Depends on case	+	+	+/-
Hack & encrypt/destroy	+	+	-	Depends on case	+	+	+

Table 3: Properties of the hack

5.2.4 Criminal data distortion

Because the aim of this thesis is to find enforcement methods that can be used for disruptive measures, respondents also thought of creative methods to reach that goal. A cybercrime expert came up with the following idea: what if the police could send dummy data to criminal systems, e.g. loads of reactions to spam mailings, to disrupt the criminal business process? If a criminal receives ten fake reactions for every genuine reaction to a spam mail, this will greatly increase his workload. The same could be done with phishing websites: if the police would fill in loads of fake credentials, the criminals couldn't distinguish real ones from fake ones. It could also be used on criminal forums and marketplaces (those on TOR as well): since many sites use a reputation system, fake reviews or forum messages could disrupt the workings of these criminal websites.
This is an interesting method that offers opportunities to disrupt criminal processes on the lighter side of the spectrum.

Properties of criminal data distortion

This method would probably not cause collateral damage in the form of overloads. The amount of data sent over the Internet is relatively small, so networks of third parties would not be overloaded.
Privacy intrusion is very low, because no systems are entered and no information is collected. However, privacy could be impaired when access to a criminal forum requires an invitation and therefore relationship with an existing member.
When carried out as described above, data distortion does not violate freedom of speech. It can be seen as "throwing sand into the criminal machine", but does not violate freedom of speech in any way. It is important however, to clearly define what is and what isn't meant with "criminal data distortion". When police interpret the term too broad, there is a risk that websites that are not purely criminal are targeted.
Police officers could easily organize this method without needing the help of third parties.
The downside will probably be the feasibility and effectiveness of the method. In case of phishing websites, it will be a challenge to find out about the phishing campaign on time; the websites are mostly online for a few hours/days, and it's very hard to detect all of them.
In case of marketplaces and criminal forums: a lot of these are underground and for example invitation only and to get there will possibly require an undercover trajectory, which is an extensive operation in the Netherlands.
Apart from that, there is a chance that criminals find out methods to counter the data distortion strategy.

	Proportionality		*Legality*		*Legitimacy*	*Practical usability*	
	Collateral Damage	Predict-ability	Privacy Intrusion	Violation Freedom of speech	Reliance on third parties	Feasi-bility	Effective-ness
Criminal data distortion	+	+	+	+	+	+/-	+/-

Table 4: Properties of criminal data distortion

5.2.5 Discarded methods

A number of methods that emerged during the interviews were discarded from the list of potential enforcement methods in cyberspace. This happened for various reasons: the method clearly doesn't concern 'enforcement', the method is clearly disproportionate, or the method is not controlled by the Dutch police but by a third party instead. The discarded methods are: IP hijack, hack and takeover, virus, Internet filtering/censoring, Internet throttling by Internet Service Providers, ARP poisoning and domain name takedown.

The **IP-Hijack** (also known as BGP hijack) exploits the Border Gateway Protocol (BGP). BGP is the protocol that is used by all the bodies that make up the Internet to decide where Internet traffic must be sent.
It exchanges routing and reachability information between Autonomous Systems (AS) on the Internet. Every intermediate AS router autonomously decides a routing policy inside the network. An AS could be for example an Internet Service Provider, a university or a corporate network (Leyes, 2015). The IP hijack lures Internet traffic for a certain website by advertising a fast route to that website. After choosing this route, it turns out that it is a dead end, thus the traffic is blocked.
The attack became widely known after Pakistan used it to block its citizens from YouTube. On government orders, Pakistan Telecom started advertising a (false) fast route to the YouTube IP, effectively hijacking traffic to the website. However, not only Pakistani visitors were hijacked, but people from Germany, China, the US, Russia, the UK and Australia as well. The duration of the outage depended on the location of the visitor, varying from one hour and forty minutes to roughly two hours (dyn research, 2008, gigaom.com, 2008). A respondent explains:

"So what you can do: if you announce that a specific IP address is accessible through you, you can pull all the traffic to you. If you subsequently throw that traffic away, you make the website with that IP unreachable." Cyber Crime expert

Where it does become difficult, is the effectiveness of the IP hijack. The IP Hijack targeted on one IP address would lead to very little success in practice. Internet infrastructure experts indicate that the policy on Internet exchanges is so that they only accept blocks from 256 addresses.

"It doesn't concern just one IP address, because BGP routing works with a /24, i.e. a block of 256 addresses. If you do it with one IP address, it will be ignored by an Internet exchange. They filter by blocks of 256 addresses, otherwise the routing tables of the Internet become too big. So with one IP it is simply not working, they won't see you." Internet infrastructure expert

If a whole block of 256 IP addresses must be hijacked, it is a different story. The clientele of a hoster or Internet Service Provider can be quite diverse and interwoven through the server network. So unless you know extremely well that the complete IP block contains criminal content, the method does a lot of collateral damage.
However, according to a respondent, some hosters have a multitude of IP blocks in use themselves. When all these IP addresses contain illegal stuff, then you could consider hijacking them all, even though there are 256. Then you have a chance that for example one IP address is a child porn site, the other is a weapon site, etcetera. Another expert puts this into perspective and indicates that this chance is very small. He does not believe that a hoster says: this is our dark corner and there are all the bad guys. Because of these obstacles we the IP Hijack is classified as poorly feasible.

The results of an IP hijack are also difficult to predict. It is hard to make an estimate: do we only touch Dutch territory, or half the world? You have very little control over who does something with the route information. The decisions that the routers make ultimately depend on what their administrators have set up, you have no control over that. Another comment that respondents have on the use of the IP hijack, is the damage it does to a fundamental element for the Internet, namely trust. The principle of BGP routing is also based on it. If you start tampering with that you possible damage the entire Internet, because the community loses trust.
The IP hijack is discarded because the hijack on a single IP address is not feasible and a hijack of 256 addresses would be disproportional and difficult to predict.

The **hack & takeover** could be interesting for law enforcement, but goes further than the "force" referred to in this thesis. The force ends after the hack, and is then succeeded by investigation, during the "takeover". It has already been applied in investigations, for example on a child porn site on TOR. In Australia, the administrator of a child porn website with 45,000 members was arrested. Then the Australian police and the FBI ran that website for half a year, to identify the members of the child porn forum (Volkskrant, 2015). This method is interesting but it does not fit with our research goal: we are looking for alternatives to investigation.

A respondent also mentioned the **computer virus** as potential cyber enforcement method. He gave an example of a police virus that spreads over the Internet and deletes all child pornography images on infected computers. Viruses are a special category; they are defined as *"parasitic programs that copy itself to other programs in order to infect additional computers."* (Sikorski & Honig, 2012, p. 4). Viruses are known to spread very quickly. This means that not only suspects could get a police virus on their computer, but also many random citizens. In addition to that: source codes of viruses can be copied and adapted by people with bad intentions. The police virus described above could for example be adjusted so that it does not remove child pornography of computers, but family snapshots, or that it places child pornography on computers. In summary: the virus is unpredictable, disproportionate and risky, thus not an interesting potential cyber enforcement method.

"So somebody has already mentioned the virus? Then I am also thinking about Stuxnet, for example. Surely that is a kind of ultimate instrument, you can destroy a lot with that, even the hardware. That is a step too far, for secret services, but certainly for the police." Digital civil rights expert

A **filter/Internet censorship** was also mentioned. It was described as *"access providers to block certain things so that they become inaccessible'*. So this is not the Internet shutdown on the side of the content provider to get a website off the air, but letting the access provider censor certain content or websites. Only service providers could carry out this action, with the police on the sidelines. It would therefore not truly be a police enforcement method. Secondly, this method is so generic that it could be seen as (preventive) censorship rather than a (reactive) enforcement method.
In 2008, a study into such a filter was already carried out by Stol, Kaspersen, Kerstens, Leukfeldt & Lodder, specifically focusing on child pornography. It turned out that if you want to block child pornography structurally on the basis of IP addresses or domain names (crude methods), a structural level of over blocking would also be created. Other, more precise filtering methods, on the basis of URL's or Deep Packet Inspection, do not create over blocking, but would slow down Internet traffic considerably, according to experts. A combination of both filtering types could be feasible (Stol et al., 2008, p. 148). However, the blocking process would be prior to

publication/display, so it would be at odds with the fundamental right of press freedom. For these reasons the Internet filter/censor is not seen as a potential cyber enforcement method.

The next method that was mentioned is the **"throttling" of Internet traffic** by Internet Service Providers. By throttling, you slow down the traffic: there is still a connection, but it is incredibly slow. It is a little less blunt than a (D)DoS attack, but the bad guy would need an hour to get to the criminal sites. It is more of a delay method than a means of force and the police cannot deploy it, only Internet providers.

Another suggestion was **ARP poisoning**, described by a cyber security expert as follows: *"To use this method, your system physically needs to be in the same server rack as your target machine, since you need to be on the same Internet switch. Subsequently, you focus on layer two, the layer of MAC addresses, in which you see ARP traffic from the target machine. Then you throw in packets from your system saying that the MAC address of the target machine has changed to yours, and then you will receive the data that were intended for the target machine."*
To use this technique, you need to know the physical location of the target machine and you need the ability to place your own server in the same rack. If that would be the case, it would be a lot easier to go to that location and seize the machine. The method would be more interesting for wiretapping/eavesdropping than as a cyber enforcement method.

The last suggestion that was discarded is the **domain name takedown**: taking a domain name offline. This can be done by ensuring that certain domain names can no longer resolve on the root name servers, so that people who click on it just get a blank screen. If people still want to visit the website, they need to find its IP address, and not many people know that. So if you want a site to be down for a while, this can be an interesting option. This technique does not cause collateral damage, provided that it is a whole site behind a domain that needs to be taken offline. The idea behind it is the same as a Notice and Takedown, only you go one step higher. The registrars, those who have registered the domain, settle the Notice and Takedown. But there are many registrars on the Internet, which makes it fairly difficult. If you wanted to do a domain name takedown via the organization that manages the country code top-level domain registry, for example .com or .nl, you could do it through one party.
For this action , you do need the cooperation of the organizations that manage domain names, for example ICANN or SIDN. The police cannot take the websites offline themselves. So here we can say as well: it is an interesting idea, but it is not a police enforcement method in cyberspace.

5.3 Comparison of the potential enforcement methods

This section is about the characteristics of the potential enforcement methods in cyberspace: what are their properties of and how do they relate? In the previous chapters, the enforcement methods were characterized as follows:

Concept ▸	*Proportionality*		*Legality*		*Legitimacy*	*Practical usability*	
Attribute(s) ▸ Method ▾	Collateral Damage	Predict-ability	Privacy Intrusion	Violation Freedom of speech	Reliance on third parties	Feasi-bility	Effective-ness
(D)DoS attack on high layer	+	+/-	+	Depends on case	+	+/-	+/-
Internet shutdown (UMTS/WiFi)	Varies	+	-	-	+	+	+
Hack & shutdown	+	+	-	Depends on case	+	+	+/-
Hack & encrypt/destroy	+	+	-	Depends on case	+	+	+
Criminal data distortion	+	+	+	+	+	+/-	+/-

Table 5: Properties of potential enforcement methods

After classifying and weighing all the enforcement methods that were mentioned by the respondents, we end up with four potential enforcement methods in cyberspace: high layer (D)DoS attack, UMTS/WiFi Internet shutdown, hack (in three combinations) and criminal data distortion. These methods all meet the requirements that were set in the beginning of the chapter: they can be used proportional, could be legitimately deployed by the police themselves, are practically usable for enforcement/disruption, and are pro-active/reactive methods. The classification system shows what the weaker and stronger attributes of the methods are. Due to their different nature, it is not possible to make a "best pick". It depends on the situation what method is the best choice. The UMTS/WiFi Internet shutdown is the stranger in our midst: it is the only method that reaches its target by air and not by an Internet connection. It is also a method that has limited possibilities. To deploy this Internet shutdown, a physical location of the target is required, but in most cybercrime cases that knowledge is missing. Therefore it will not be an interesting method to disrupt criminal phenomena such as (D)DoS attacks or illegal trade on TOR. This enforcement method belongs more in the realm of counter terrorism units, e.g. a UMTS signal jammer to use in a hostage situation. The Internet shutdown is seen as an infringement of basic rights so it would need a legal basis to deploy it.

The other three methods all reach their target by Internet and offer possibilities for criminal disruption. A considerable difference between the high layer (D)DoS attack, criminal data disruption and hack is that the last is seen as a significant intrusion of a basic right: privacy. That means new legislation is needed to meet the legality principle and to use the hack purely for disruption. At first sight it seems that the high layer (D)DoS attack and criminal data disruption do not violate basic rights and can possibly be deployed using article 3 of the police law as justification. A legal expert should judge this when a specific case arises.

5.4 Pre-conclusion

In this chapter, four potential enforcement methods in cyberspace were distinguished. The first section of the chapter explored the general circumstances in which a method could be used. The respondents agree that, following the example of physical enforcement, officers should be instructed properly before they can use enforcement methods in cyberspace.

The decision to choose a certain method in future situations, while using the concepts of proportionality and subsidiarity, will entail both physical and digital options. It is possible that police start with a digital method, then a physical, and follow up with a digital again. Collateral damage is something that should be kept to a minimum, but it cannot be avoided at all times.

The respondents provided a surplus of information that enabled us to classify and select the methods. In the beginning of section 5.2, the requirements for potential enforcement methods were defined. Many methods that were mentioned by respondents did not meet these requirements and were discarded. We ended up with four potential enforcement methods: high layer (D)DoS attack, UMTS/WiFi Internet shutdown, hack (in three combinations) and criminal data distortion.

6. Discussion

Combining the use of force by police officers with the cyberspace domain is a daring cocktail. The cyberspace and Internet community can be characterized as autonomous, liberal and in some places anarchistic; writing about police enforcement methods in cyberspace could be interpreted as an attack on Internet freedom. For that reason, it is utterly important to explain precisely why this thesis was written. As cyberspace becomes so entangled with all other aspects of our lives, it is not possible anymore to see it isolated from the physical world. Cyberspace has become part of our society. The police have the task to effectively enforce law and order, and provide assistance to those in need. Law and order and people in need of assistance also exist in cyberspace. That is why the Dutch police should be equipped with suitable tools to perform their task. Freedom and trust are crucial for the survival of the Internet that we all love. That is exactly the reason why any attempt to start using enforcement methods in cyberspace should be sensible and well thought out. That is why this analysis was needed, to separate sense from non-sense and to provide a realistic picture of the possibilities and impossibilities of law enforcement in cyberspace. This master thesis is only the beginning: it is a starting point for further research and for discussions amongst policy makers, police chiefs, experts and citizens. There is still a lot to be done before law enforcement in cyberspace reaches maturity.

One important limitation of this thesis is the absence of an in-depth analysis of sovereignty issues and jurisdiction when using enforcement methods in cybercrime. These are relevant issues, because a large portion of cybercrime comes from abroad (e.g. the real problematic bulletproof hosting providers). It was a deliberate choice to leave the international aspect out of the research because it would make this thesis too extensive. Again, this analysis should be seen as a first step. Further research is needed to determine possibilities to use enforcement in situations where location of data is international and diffuse.

Another limitation of this study is the lack of research into the risks that law enforcement in cyberspace could pose, regarding acts of retaliation. Targets of law enforcement actions could counter the attack by trying to hack or (D)DoS the police. The extra risks this poses for the cyber security of police infrastructures should be considered. It will also depend on the targets that are chosen. Attacking child pornography websites would probably pose little retaliation risk since the small support base they have in society, but for dark net markets this could be different. Hacktivist groups such as Anonymous are known for cyber attacks against institutions that antagonize them (Coleman, 2014).

Lastly, this thesis is specifically aimed at police enforcement methods. Off course, policing is broader than that. Other policing models, as well as public-private partnerships are just as important to combat cybercrime and the ideas in this thesis should be seen as a supplement, not a substitute.

7. Conclusions and recommendations

7.1 Conclusions

This thesis started with the police task "*carrying out the effective enforcement of law and order and providing assistance to those in need*" and the authority to use legitimate force that Dutch police possess. Police officers have a number of instruments at their disposal to apply force and police organizations have specialized riot police units.
A literature study showed that it took a long time for Dutch police to obtain their central role in the application of physical force. Before that, the military gave assistance when needed, resulting in disproportionate and deadly actions.
To prevent a similar scenario for enforcement in cyberspace, the issue should be discussed in due time.
But the police authority to use legitimate force hasn't been associated with cyberspace yet; police law and instructions don't say anything about it. This is remarkable, because "cyber" became an undeniable aspect of contemporary live. People are always online and the importance of our actions and our communication in cyberspace equal those in the physical world.
By studying (case) law and conducting interviews we concluded that the police authority to use legitimate force is also applicable to cyberspace. All respondents, from public to private sector, from universities to a digital civil rights organization acknowledged this. However, police currently lack enforcement methods. They do conduct criminal investigations, but many types of crimes that (wholly or partly) take place in cyberspace, pose difficulties for investigators. Locations of criminals in cyberspace and in the physical world are hidden or spoofed, identities are false, and tracks and logging are quickly gone. This relates to many types of crime, for example (D)DoS attacks and illegal trade on TOR (both described in chapter 2), child pornography, terrorism and e-fraud.
Undoubtedly new types of (cyber) crime will follow in the future. Due to the difficulties of investigation and prosecution, it can be interesting to look at the strategy of disruption: trying to influence circumstances to prevent and disrupt crime. Combining this strategy with potential enforcement methods in cyberspace confronts us with many legal and ethical issues.
The first legal issue is the authority to "*enter an automated work that is in use by the suspect, with or without a technical tool*", also known as the hack. This is introduced in the proposed 3rd law on computer crime, in the code of criminal procedure. It is meant for the prosecution of a person and cannot be used for purely disruptive purposes. Disruption can be a second goal in addition to prosecution, but not a first. To use the hack for disruption of criminal processes, another legal foundation is needed. This is probably the same for other enforcement methods, but opinions about the legal foundations that are needed differ. Some respondents believe that the existing article 3 from the Dutch Police Law is enough justification to use these methods, whereas others think some adjustments in law are needed. It will probably depend whether or not the method causes more than a minor infringement of the basic rights of the person, the legality principle.
The most probable place in the law for cyber enforcement methods will be the Police Law, article 7, and the Official instructions for police, royal constabulary and other investigation officers. Another legal challenge is the international aspect of cybercrime. Since a large portion of cybercrime comes from abroad, there is a big chance you violate sovereignty and jurisdictions of other states when using an enforcement method. This is the same for the TOR web, with one difference: on TOR you initially have no idea where hidden services are located, so the

jurisdiction is unknown. Only after you hack the website you can see where it is located. The proposed cybercrime law in the Netherlands describes this issue as follows: if you cannot find a location, then you can take a first action.

Enforcing the law in cyberspace confronts us with ethical and societal issues as well. Firstly, we should constantly think about the impact that methods have on society, e.g. what freedoms can be taken in order to take certain measures. Just as happened with enforcement in the physical world, the police needs to find a kind of balance. To let this process run smoothly, the enforcement methods should be used transparently and the police must be able to give explanation. Extra caution is needed when certain enforcement methods might bring freedom of speech at risk. If the police systematically disrupted certain types of forums, citizens could no longer express a certain opinion, and that would be a problem. Another major consideration is the potential loss of trust that people have in the Internet. The Internet, for example BGP routing, functions on the basis of trust. Certain enforcement methods could have a negative influence on that. These things should always be kept in mind when considering deploying certain enforcement methods. Other important principles are proportionality and subsidiarity. Proportionality means that the amount or type of force that is applied should be proportional in risk and effects considering the intended purpose. If a method causes a severe amount of collateral damage, that could be reason to avoid it. Subsidiarity means that there should not be less intrusive options to reach the intended purpose. The decision to choose a certain method in future situations will entail both physical and digital options. It is possible that police start with a digital method, then a physical, and follow up with a digital one again.

In the last chapter of this thesis, a list of potential enforcement methods in cyberspace and their characteristics was composed. This list contains the following four methods: high layer (D)DoS attack, UMTS/WiFi Internet shutdown, hack (in three combinations) and criminal data distortion. The hack provides access to the target system, whereas the other methods only influence the traffic to or from the target system. For that reason it is seen as a significant privacy intrusion. The UMTS/WiFi Internet shutdown takes away an essential means of communication. Therefore it is also seen as a privacy intrusion and a violation of free speech: without an Internet connection it is almost impossible nowadays to express yourself.

The other two methods, high layer (D)DoS attack and criminal data distortion do not seem to violate basic rights at first sight and can possibly be deployed using article 3 of the police law as justification. However, expectations regarding their effectiveness differ. (D)DoS protection on criminal websites and other counter strategies could render their effect useless. Further empirical research can provide more clarity.

7.2 Recommendations

The above conclusions lead to the following recommendations:

- To create clarity, the legislator should propose an amendment of police law by adding cyber enforcement methods to it. This could be done with an addition to article 7 of the Dutch Police Law making clear that the capability to use force also applies to cyberspace. In the Official instructions for police, royal constabulary and other investigation officers, specific enforcement methods and instructions could be added. The latter is especially important for the hack as purely disruptive enforcement method, because current and proposed cybercrime law does not yet allow for that.

- Further empirical research should be conducted on the effectiveness of the two methods from this thesis that seem to comply the legality principle: high layer (D)DoS attacks and criminal data distortion. In the beginning that could be done with pilot experiments, measuring the effectiveness of the two methods to disrupt criminal phenomena in cyberspace. Before using a method in a specific case, a legal expert should judge whether it complies with the legality principle.
- Further research should be conducted on cyber enforcement against targets that are in other jurisdictions, when national sovereignty could be violated. A high percentage of cybercrime comes from abroad, so it should be assessed what the possibilities and legal challenges are.
- Further research should be conducted on police cryptoware: locking the data on a system by using encryption. Respondents specifically mentioned this as an interesting method to combine with a hack. It would be a sort of digital equivalent of the handcuffs. Further research is needed to assess the possibilities of this tool. The study should also find out whether cryptoware has a bad reputation because criminals use it and if that would change when police start using it.
- Before deploying cyber enforcement methods, Dutch police should perform an internal assessment to determine the extra cybersecurity risks (e.g. retribution attacks) for the police organization that enforcement in cyberspace could entail and whether the organization is protected against that.

References

Adang, O.M.J., Bierman, S.E., Jagernath-Vermeulen, K., Melsen, A., Nogarede, M.C.J., van Oorschot, W.A.J. (2009). Boven de pet? Een onderzoek naar grootschalige ordehandhaving in Nederland. Amsterdam, The Netherlands: Reed Business. Retrieved from https://kennismag.politieacademie.nl/05/Documents/boven%20de%20pet.pdf

Baran, P. (1964). On Distributed Communications: Introduction to Distributed Communications Networks. Santa Monica, CA: RAND Corporation. Retrieved from http://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf

Baraniuk, C. (2014). Nest thermostat acquisition is Google's home invasion. *New Scientist*. Retrieved from http://www.newscientist.com/article/mg22129535.200nestthermostatacquisitionisgoogleshomeinvasion.html?full=true&print=true

Bauman, Z. & Donskis, L. (2013). Moral Blindness: The Loss of Sensitivity in Liquid Modernity . Cambridge, UK: Polity Press

Bilge, L. & Dumitras, T. (2012). Before we knew it. An Empirical Study of Zero-Day Attacks In The Real World. In Yu, T. (Ed.), Proceedings of the 2012 ACM conference on Computer and communications security, (p. 1). NY, USA: ACM New York. Retrieved from https://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf

Bleijendaal, R., Naeyé, J., Chattellon, P. & Drenth, G. (2008). Kracht van meer dan geringe betekenis. Deel A: Politiegeweld in de basispolitiezorg. Den Haag, The Netherlands: Reed Business.

Bradley, J., Loucks, J., Macaulay, J., Noronha, A. & Wade, M. (2015). Digital Vortex. How Digital Disruption is Redefining Industries. Retrieved from http://www.imd.org/uupload/IMD.WebSite/DBT/Digital_Vortex_06182015.pdf

Breukers, J. (n.d.). De Politiegeschiedenis in Hoofdlijnen. Retrieved from http://www.politiemuseum.nl/UserFiles/File/politiegeschiedenis_op_hoofdlijnen.pdf

Brunner, G. (2015). The ultimate guide to staying anonymous and protecting your privacy online. Retrieved from http://www.extremetech.com/internet/180485-the-ultimate-guide-to-staying-anonymous-and-protecting-your-privacy-online

Burkens, S. (2014). *Art. 13b Opiumwet. Handhaven aan de grenzen van herstel* (master thesis, University of Amsterdam, the Netherlands). Retrieved from http://njb.nl/Uploads/2015/7/scriptie-NJB27.pdf

Castells, M. (2010). *The Rise of the Network Society, The Information Age: Economy, Society and Culture Vol. I.* (2nd ed.) Cambridge, MA; Oxford, UK: Blackwell. Retrieved from https://deterritorialinvestigations.files.wordpress.com/2015/03/manuel_castells_the_rise_of_the_network_societybookfi-org.pdf

Centraal Plan Bureau (2016). Risicorapportage Cyberveiligheid Economie. Retrieved from http://www.cpb.nl/sites/default/files/omnidownload/CPB-Notitie-6juli2016-Risicorapportage-cyberveiligheid-economie.pdf

Centre for Crime Prevention and Safety (2015) Bestaande Bouw. Handboek Politiekeurmerk Veilig Wonen. Retrieved from http://www.hetccv.nl/binaries/content/assets/ccv/webwinkel/pkvw/pkvw_bb2015_online2.pdf

Chaum, D. (1981). Untraceable Electronic Mail, Return Adresses, and Digital Pseudonyms. Communications of the ACM, vol. 24, no. 2. Retrieved from: http://www.freehaven.net/anonbib/cache/chaum-mix.pdf

Cohn, N. (2012). The power of navigation and real time traffic: reduced congestion + reduced co2 emissions = smart cities. Retrieved from http://www.eurobench.com/Forum/Upload/2013/7026310.pdf

Coleman. G. (2014). *Hacker, Hoaxer, Whistleblower, Spy. The many faces of anonymous*. London, United Kingdom: Verso. Retrieved from http://ijoc.org/index.php/ijoc/article/download/3838/1333

Conings, C. & Oerlemans, J.J. (2013). Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?, *Computerrecht*, 2013, No. 1, p. 23-32.

Dekker, N. (2014, October 21). Politie moet excuses maken na gewelddadige arrestatie pietendemonstranten. *AD*. Retrieved from http://www.ad.nl/ad/nl/32605/Dordrecht/article/detail/3772594/2014/10/21/Politie-moet-excuses-maken-na-gewelddadige-arrestatie-pietendemonstranten.dhtml

Dingledine, R., Mathewson, N. & Syverson, P. (2004). Tor: The Second-Generation Onion Router. In *Proceedings of the 13th conference on USENIX Security Symposium* (pp. 21-21). San Diego, CA: USENIX.

Domenie, M.M.L., Leukfeldt, E.R., van Wilsem, J.A., Jansen, J. & Stol, W. Ph. (2013). Slachtofferschap in een gedigitaliseerde samenleving. Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit. The Hagua, The Netherlands: Boom Lemma. Retrieved from https://www.nhl.nl/sites/default/files/files/Bedrijf-en-Onderzoek/Lectoraten-Documenten/Slachtofferschap%20in%20een%20gedigitaliseerde%20samenleving.pdf

Drenth, G., Naeyé, J. & Bleijendaal, R. (2008). *Kracht van meer dan geringe betekenis. Deel B: Sturing en toetsing van de politiële geweldsbevoegdheid.* Den Haag, The Netherlands: Reed Business.

Einarsen, T. (2012). *The Concept of Universal Crimes in International Law*. Oslo, Norway: Torkel Opsahl Academic EPublisher.
Retrieved from https://www.fichl.org/fileadmin/fichl/documents/FICHL_14_Web.pdf

Europol. (2015). Botnet Taken Down Through International Law Enforcement Cooperation. Retrieved from https://www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-cooperation

Evans, D. (2010). The Internet of Everything. How More Relevant and Valuable Connections Will Change the World. Retrieved from Cisco website: https://www.cisco.com/web/about/ac79/docs/innov/IoE.pdf

Farwell, J.P. & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War, *Survival*, Vol. 53, No. 1, pp. 23-40

Fidler, M. (2015). Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis. I/S: A journal of law and policy for the information society, Vol. 11, No. 2, p. 406. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2706199

Fijnaut, C. (2008). *A History of the Dutch Police.* Amsterdam, The Netherlands: Boom.

Goldschlag, D., Reed, M. & Syverson, P. (1999). Onion Routing for Anonymous and Private Internet Connections. *Communications of the ACM*, 42 (2), p. 39-41. Retrieved from http://www.onion-router.net/Publications/CACM-1999.pdf

Groenhuijsen, M. S., & Wiemans, F. P. E. (1989). Van electriciteit naar computercriminaliteit. (Monografieën strafrecht; No. 9). Arnhem, The Netherlands: Gouda Quint. Retrieved from https://pure.uvt.nl/portal/files/647071/ELECTRIC.PDF

Guion, L., Diehl, D.C., & McDonald, D. (2001). Conducting an In-depth Interview. Retrieved from http://greenmedicine.ie/school/images/Library/Conducting%20An%20In%20Depth%20Interview.pdf

Herzberg, A. & Shulman, H. (2014). DNS Authentication as a Service: Preventing Amplification Attacks. In C.N. Payne, Jr. (Ed.), *Proceedings of the 30th Annual Computer Security Applications Conference* (pp. 356-365). New York, NY: ACM.

Kaspersen, H.W.K. (2007). Cyber crime in historisch perspectief. In B.J. Koops (Ed.), *Strafrecht en ICT* (pp.13-22). The Hague, NL: SDU.

Kleinrock, L. (1961). Information Flow in Large Communication Nets. RLE Quarterly Progress Report. Retrieved from http://www.lk.cs.ucla.edu/data/files/Kleinrock/Information%20Flow%20in%20Large%20Communication%20Nets0.pdf

Koetsenruyter, L. & van den Outenaar, E. (2014, December 6). Waarom vallen al die merkzaken om? *De Volkskrant.* Retrieved from http://www.volkskrant.nl

Krebs, D. (2010, November 9). Body armor for bad websites. Retrieved from Krebsonsecurity website: http://krebsonsecurity.com/2010/11/body-armor-for-bad-web-sites/

Kwon (2015) Circuit Fingerprinting Attacks: Passive Deanonymization of Tor Hidden Services. Retrieved from https://people.csail.mit.edu/devadas/pubs/circuit_finger.pdf

Koops, E. J. (2014). Cybercriminaliteit. In S. van der Hof, A. R. Lodder, & G. J. Zwenne (Eds.), *Recht en computer,* zesde druk. (pp. 213-241). Deventer, NL: Kluwer Retrieved from https://pure.uvt.nl/ws/files/1579089/Koops_Cybercrime_2014def.pdf

Leiner, *B. M.,* Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Robers, L. G. and Wolff, S. *(*2009). *A* brief history of the internet. *Computer Communication Review.* Vol. 39, No. 5, pp. 22-31. Retrieved from http://www.cs.ucsb.edu/~almeroth/classes/F10.176A/papers/internet-history-09.pdf

Licklider, J.C.R. & Clark, W. (1962). On-Line Man Computer Communication. *AFIPS*, 1962, Managing Requirements Knowledge, International Workshop on, Managing Requirements Knowledge, International Workshop on 1962, pp. 113, doi:10.1109/AFIPS.1962.24 Retrieved from http://memex.org/licklider.pdf

McCoy, D., Bauer, K., Grunwald, D., Kohno T. and Sicker, D. (2008). Shining Light in Dark Places: Understanding the Tor Network. In N. Borisov & I. Goldberg (Eds.), Privacy Enhancing Technologies. 8th International Symposium, PETS 2008 Leuven, Belgium, July 23-25, 2008 (pp. 63-76). Retrieved from http://freehaven.net/anonbib/cache/mccoy-pet2008.pdf

Mc Guire & Dowling, (2013). Cyber crime: A review of the evidence. Research Report 75. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

M.E. ingezet bij actie Greenpeace tegen kerntransport Borssele. (2011, June 7). *Omroep Brabant.* Retrieved from http://www.omroepbrabant.nl/?news/156328992/ME+ingezet+bij+actie+Greenpeace+tegen+kerntransport+Borssele.aspx

Meershoek, A.J.J. (2012). De politiekoppel: vormgever van het geweldsmonopolie. In: P.W. Tops (Ed.), *Inleiding politiekunde (pp. 71-80)*. Apeldoorn, the Netherlands: Politieacademie. Retrieved from http://doc.utwente.nl/82817/1/Politiekoppel-2.pdf

Microsoft (n.d.). The OSI Model's Seven Layers Defined and Functions Explained. Retrieved from https://support.microsoft.com/en-gb/kb/103884

Naeyé, J. (2005). Niet zonder slag of stoot. De geweldsbevoegdheid en doorzettingskracht van de Nederlandse politie. Zeist, The Netherlands: Kerkebosch

NCSC, (2014). Cybersecuritybeeld Nederland. Retrieved from https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecuritybeeld-nederland-4/1/CSBN%2B4.pdf

NCSC, (2012). Handreiking Cybercrime. Retrieved from https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/whitepapers/handreiking-cybercrime/1/Handreiking%2BCybercrime.pdf

Nederland en Australië rollen 's werelds grootste kinderpornonetwerk op. (2015, November 25). De Volkskrant. Retrieved from http://www.volkskrant.nl/binnenland/nederland-en-australie-rollen-s-werelds-grootste-kinderpornonetwerk-op~a4194202/

Olson, P. (2012). *We Are Anonymous. Inside the Hacker World of LulzSec, Anonymous and the Global Cyber Insurgency.* New York, NY: Back Bay Books.

Onderzoek naar gebruik nekklem. (2015, July 8). *Trouw*. Retrieved from http://www.trouw.nl/tr/nl/4492/Nederland/article/detail/4097311/2015/07/08/Onderzoek-naar-gebruik-nekklem.dhtml

Perlroth, (2014). Tally of Cyber Extortion Attacks on Tech Companies Grows [Web log post]. Retrieved from http://bits.blogs.nytimes.com/2014/06/19/tally-of-cyber-extortion-attacks-on-tech-companies-grows/

Politie maakt einde aan bezetting Maagdenhuis. (2015, April 11). *De Volkskrant*. Retrieved from http://www.volkskrant.nl/binnenland/politie-maakt-einde-aan-bezetting-maagdenhuis~a3949119/

Pondsmith, M. (1988) View from the Edge - The Cyberpunk Handbook. R. Talsorian Games Inc. in Birch, D.G.W. & Buck, S.P. (1991). What is Cyberspace. Retrieved from http://cyberpunk.asia/cp_pdf.php?txt=150&lng=us

Rahimi, B. (2015). Internet Censorship in Rouhani's Iran: The " Wooden Sword". *Asian Politics & Policy*, 7 (2), pp 336-341.

Rowland. J., Rice, M. and & Shenoi, S. (2014). The Anatomy of a Cyber Power. *International Journal of Critical Infrastructure Protection, Vol.* 7, No. 2, pp. 3-11. doi: 10.1016/j.ijcip.2014.01.001. Retrieved from https://www.researchgate.net/profile/Sujeet_Shenoi/publication/259994578_The_Anatomy_of_a_Cyber_Power/links/55b501a008ae092e965581a0.pdf

Ruim 20 arrestaties bij kolencentraleprotest. (2014, June 14). *De Telegraaf.* Retrieved from http://www.telegraaf.nl/binnenland/22739924/__Arrestaties_bij_milieuprotest__.html

Sauter, M. (2014). *The Coming Swarm. (D)DOS Actions, Hacktivism, and Civil Disobedience on the Internet.* New York, NY: Bloomsbury.

Segura, V. & Lahuerta, V. (2010). Modeling the Economic Incentives of DDoS Attacks: Femtocell Case Study. In T. Moore et al. (eds.) Economic of Information Security and Privacy 2010, pp. 107-119. Springer Science+Business Media, LLC. doi: 10.1007/978-1-4419-6967-5_7. Retrieved from http://weis09.infosecon.net/files/113/paper113.pdf

Stol, W. Ph., Kaspersen, H.W.K., Kerstens, J., Leukfeldt, E.R. & Lodder, A.R. (2008). *Filteren van kinderporno op internet. Een verkenning van technieken en reguleringen in binnen- en buitenland.* Den Haag, the Nederlands: Boom.

Strikwerda, L. (2014). Virtual Acts, Real Crimes? A Legal-Philosophical Analysis of Virtual Cybercrime (Doctoral dissertation). Retrieved from http://doc.utwente.nl/92041/1/thesis_L_Strikwerda.pdf

Taneja, H. & Wu, A.X. (2014). Does the Great Firewall Really Isolate the Chinese? Integrating Access Blockage With Cultural Factors to Explain Web User Behaviour. *The Information Society*, 30 (5), pp. 297-309.

Thuiswinkel.org (2015) Nederlanders besteden in 2014 bijna € 14 miljard online [Press release]. *English: Dutch spend almost € 14 billion online in 2014*. Retrieved from https://www.thuiswinkel.org/bedrijven/nieuws/2721/nederlanders-besteden-in-2014-bijna-14-miljard-online

Turkey seizes 13 tons of drugs in international waters. (2016, January 6). *Hurriyet Daily News*. Retrieved from http://www.hurriyetdailynews.com/turkey-seizes-13-tons-of-drugs-in-international-waters.aspx?pageID=238&nID=93472&NewsCatID=359

Van der Wal, R. (2003). *Of geweld zal worden gebruikt! Militaire bijstand bij de handhaving en het herstel van de openbare orde 1840-1920.* Hilversum, The Netherlands: Verloren

Verpaalen, J.P.F. (2007). Tegenhouden. "Dient, door toepassing door de politie van grensverleggende activiteiten in het kader van het concept tegenhouden, de bestaande wetgeving te worden aangepast?" (master thesis, Open University, the Netherlands)

Voermans, W.J.M. (2011). Legaliteit als middel tot een doel, in: Controverses rondom legaliteit en legitimatie; handelingen NJV 141e jaargang Handelingen Nederlandse Juristen Vereniging. Deventer: Kluwer, pp. 1-101. Retrieved from https://www.researchgate.net/profile/Wim_Voermans/publication/254883372_Controverses_rondom_legaliteit_en_legitimatie/links/54afb9cf0cf29661a3d5d5c8.pdf

Yang, Q. & Liu, Y. (2014). What's on the other side of the great firewall? Chinese Web users' motivations for bypassing the Internet censorship. *Computers in Human Behavior,* 37 (2014), pp. 249-257. Retrieved from https://www.researchgate.net/publication/262690944_What's_on_the_other_side_of_the_great_firewall_Chinese_Web_users'_motivations_for_bypassing_the_Internet_censorship

Yar, M. (2006) *Cybercrime and Society.* London: Sage Publications.

Zetter, K. (2005). Tor Torches Online Tracking. *Wired Magazine*. Retrieved from http://archive.wired.com/politics/security/news/2005/05/67542?currentPage=all

Picture on frontpage downloaded from: http://barbwire.wpengine.netdna-cdn.com/wp-content/uploads/2014/06/keyboardweapon.jpg

Case law and parliamentary documents

Court of Amsterdam, 2 April 2009, ECLI:NL:RBAMS:2009:BH9791. Retrieved from http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2009:BH9789

Court of Limburg, 20-3-2013, ECLI:NL:RBLIM:2013:BZ5447

Court of justice Leeuwarden, 5-8-2009, ECLI:NL:GHLEE:2009:BJ4666

Dutch Government (2015a). Wetsvoorstel Computercriminaliteit 3. Retrieved from https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/23/wetsvoorstel-computercriminaliteit-iii

Dutch Government (2015b). Wetsvoorstel Computercriminaliteit 3. Memorie van Toelichting. Retrieved from https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2015/12/23/memorie-van-toelichting-wetsvoorstel-computercriminaliteit-iii/memorie-van-toelichting-deel-1-2-computercriminaliteit-iii.pdf

Dutch Government (2014). Evaluatie Nederlandse inzet in de antipiraterijoperaties Atalanta en Ocean Shield 2013. Retrieved from https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2014/09/25/evaluatie-inzet-in-de-antipiraterijoperaties-atalanta-en-ocean-shield-2013/evaluatie-inzet-in-de-antipiraterijoperaties-atalanta-en-ocean-shield-2013.pdf

Dutch government (2013). Nationale Cybersecurity Strategie 2. Van bewust naar bekwaam. Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2013/10/28/nationale-cyber-security-strategie-2

Dutch government (2012). Police law, retrieved from http://wetten.overheid.nl/BWBR0031788/geldigheidsdatum_17-09-2015

Dutch Government (1998). Legislation for the electronic highway (Wetgeving voor de elektronische snelweg). Retrieved from https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vi3agwzji6uz#p1

Dutch government (1994). Ambtsinstructie voor de politie, de Koninklijke marechaussee en andere opsporingsambtenaren. Retrieved from http://wetten.overheid.nl/BWBR0006589/geldigheidsdatum_20-09-2015#Hoofdstuk1_Artikel1

Supreme Court, 31 January 2012, ECLI: NL: HR: 2012: BQ9251. Retrieved from http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:HR:2012:BQ9251

Supreme Court, 3 December 1996, *NJ (Nederlandse Jurisprudentie)* 1997/574, pp. 3086-3094.

Supreme Court, 22 februari 1977, *NJ (Nederlandse Jurisprudentie)* 1977/288, pp. 1005-1009.

Supreme Court, 23 May 1921, *NJ (Nederlandse Jurisprudentie)* 1921/564, pp. 564-574 (concl. Jhr. van Meeuwen).

Centre for Criminality Prevention and Safety (2007). Gedragsaanwijzing, retrieved from: http://www.hetccv.nl/binaries/content/assets/ccv/dossiers/wet-mbveo/wet_mbveo_mvt_gedragsaanwijzing_ovj.pdf

United Kingdom Government (2011). The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

United Nations (1988). United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. Retrieved from https://www.unodc.org/pdf/convention_1988_en.pdf

United Nations (1982). *United Nations Convention on the Law of the Sea. Retrieved from* http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

Wetboek van Starfrecht (n.d.). Retrieved from
http://wetten.overheid.nl/BWBR0001854/EersteBoek/TitelI/Artikel2/geldigheidsdatum_10-12-2015

Wet Algemene Bepalingen (n.d.). Retrieved from
http://wetten.overheid.nl/BWBR0001833/geldigheidsdatum_10-12-2015